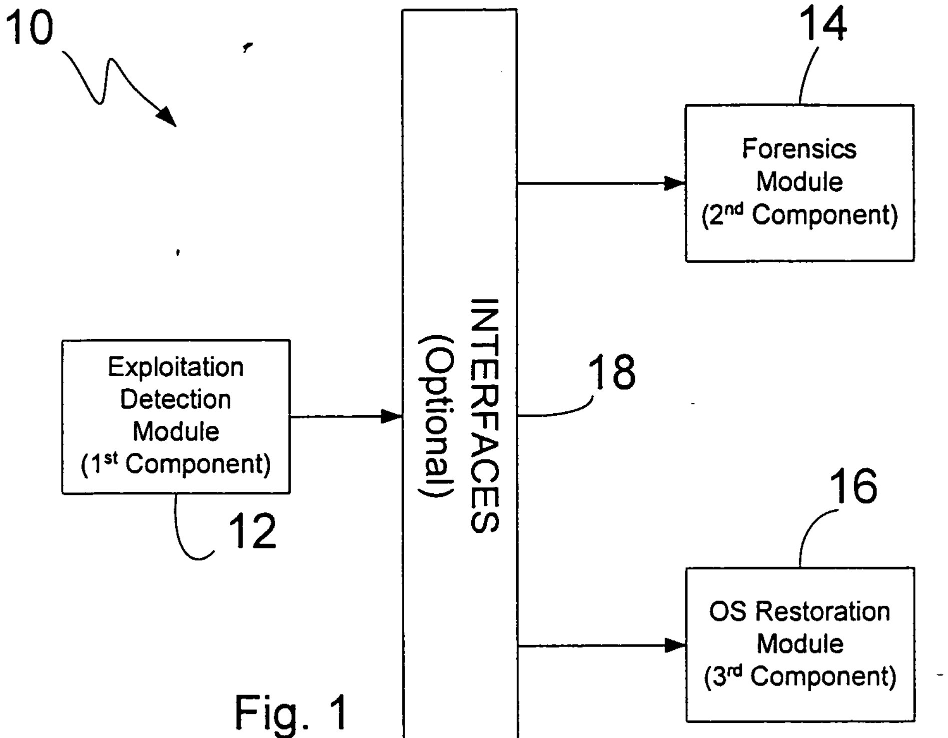

10
14
Forensics Module (2nd Component)
Exploitation Detection Module (1st Component)
INTERFACES (Optional)
18
12
16
OS Restoration Module (3rd Component)

Fig. 1

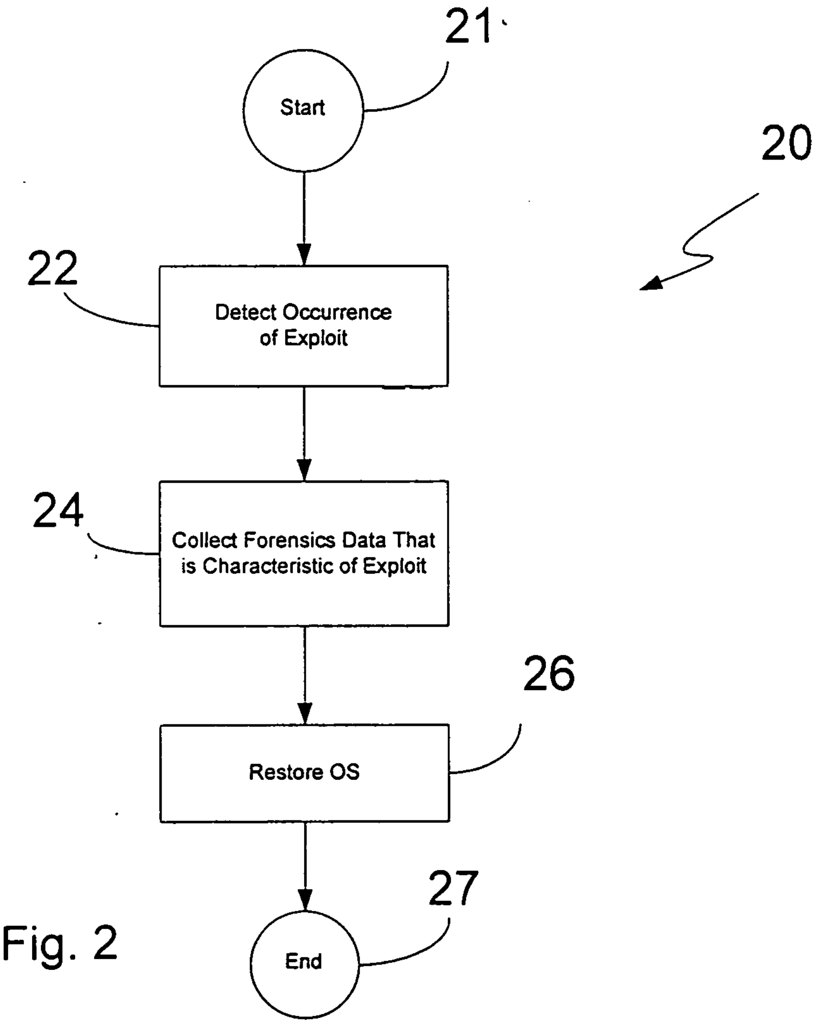

21
Start
20
22
Detect Occurrence of Exploit
24
Collect Forensics Data That is Characteristic of Exploit
26
Restore OS
27
End

Fig. 2

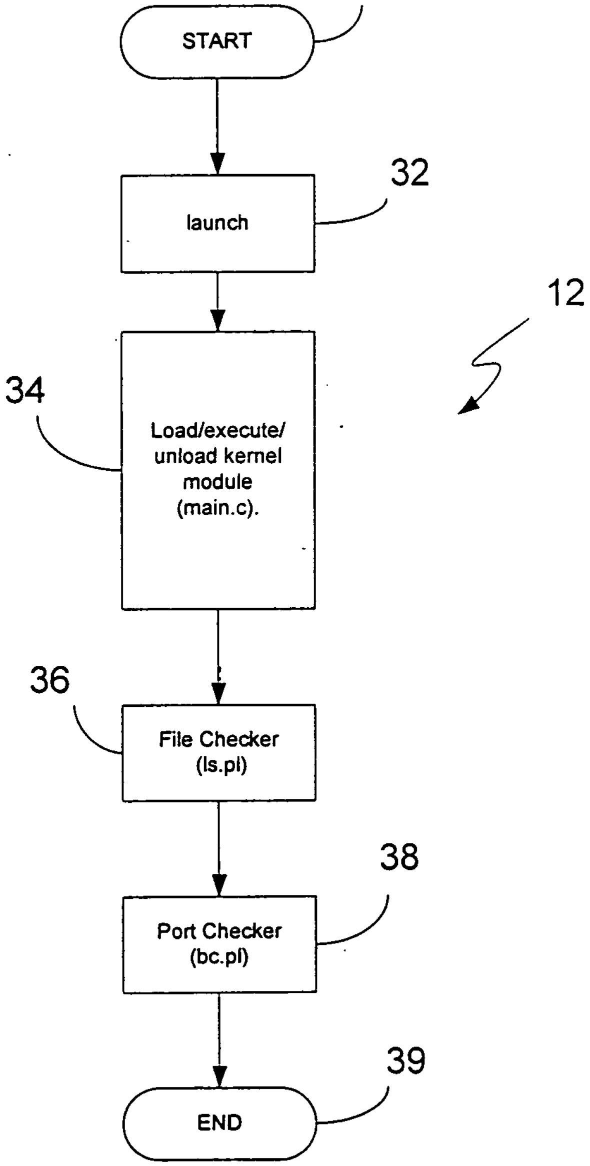


FIG. 3

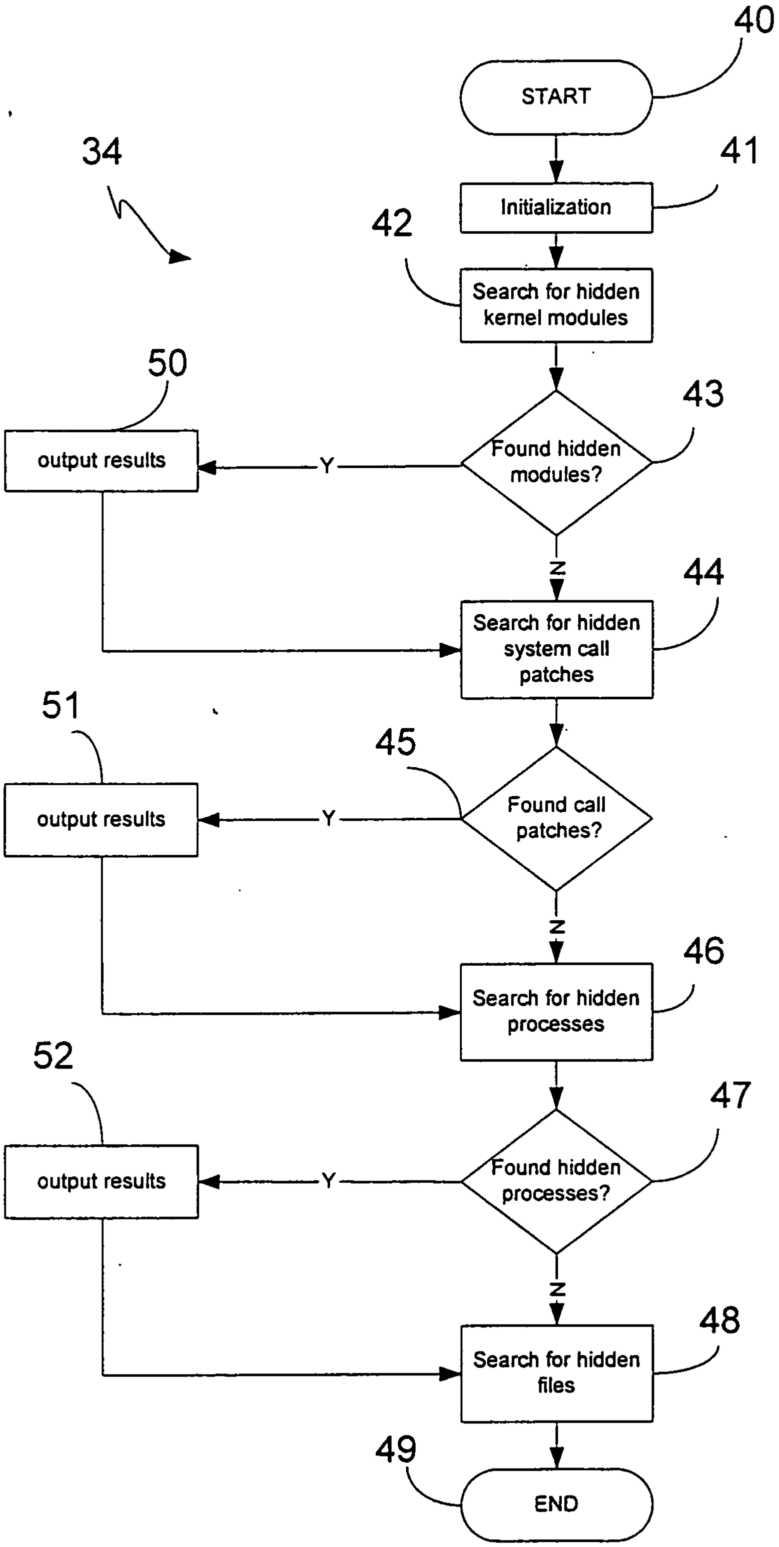

40
START
41
Initialization
34
42
Search for hidden kernel modules
50
43
output results
Y
Found hidden modules?
N
44
Search for hidden system call patches
51
45
output results
Y
Found call patches?
N
46
Search for hidden processes
52
47
output results
Y
Found hidden processes?
N
48
Search for hidden files
49
END

FIG. 4

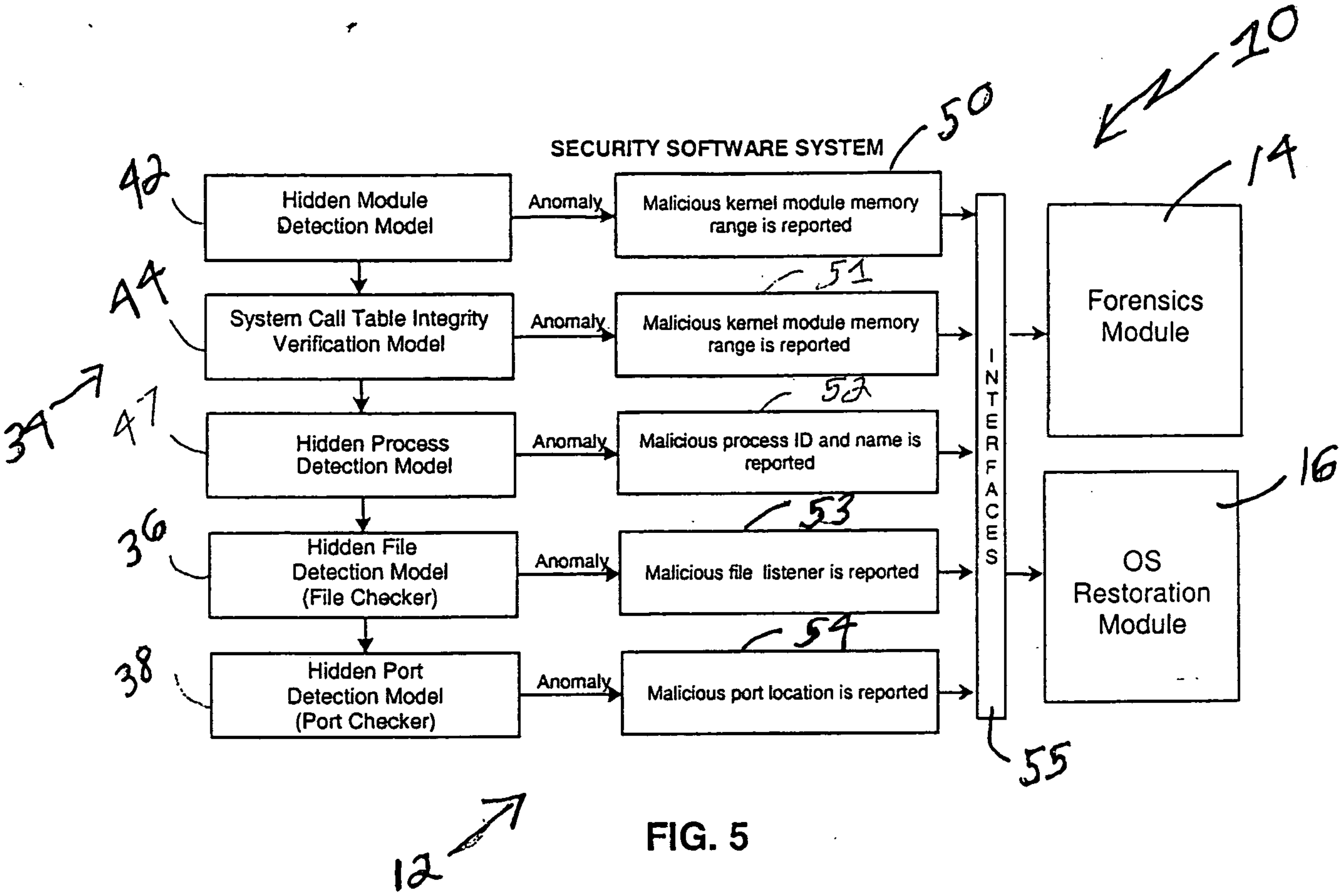

SECURITY SOFTWARE SYSTEM
10
50
42
Hidden Module Detection Model
Anomaly
Malicious kernel module memory range is reported
44
System Call Table Integrity Verification Model
Anomaly
51
Malicious kernel module memory range is reported
39
47
Hidden Process Detection Model
Anomaly
52
Malicious process ID and name is reported
36
Hidden File Detection Model (File Checker)
Anomaly
53
Malicious file listener is reported
38
Hidden Port Detection Model (Port Checker)
Anomaly
54
Malicious port location is reported
INTERFACES
55
14
Forensics Module
16
OS Restoration Module
12

FIG. 5

KERNEL MODULE HIDING
Module list before removal

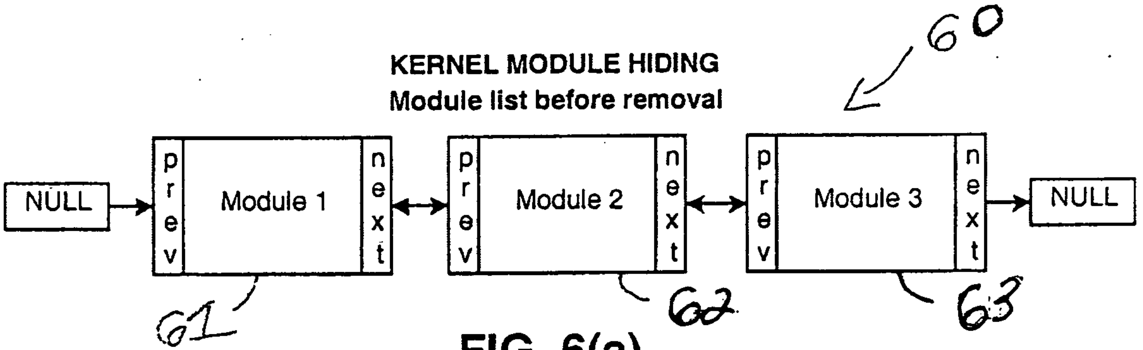


FIG. 6(a)

Module list after hacker technique for removal

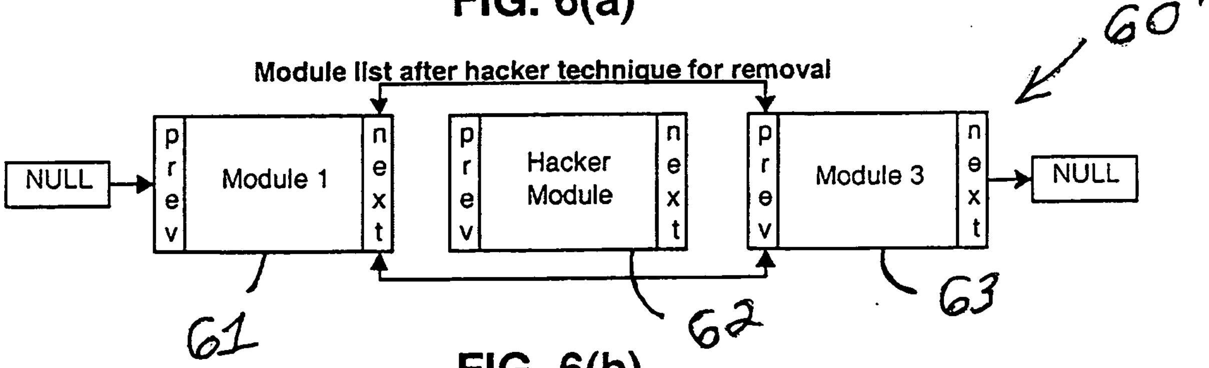


FIG. 6(b)

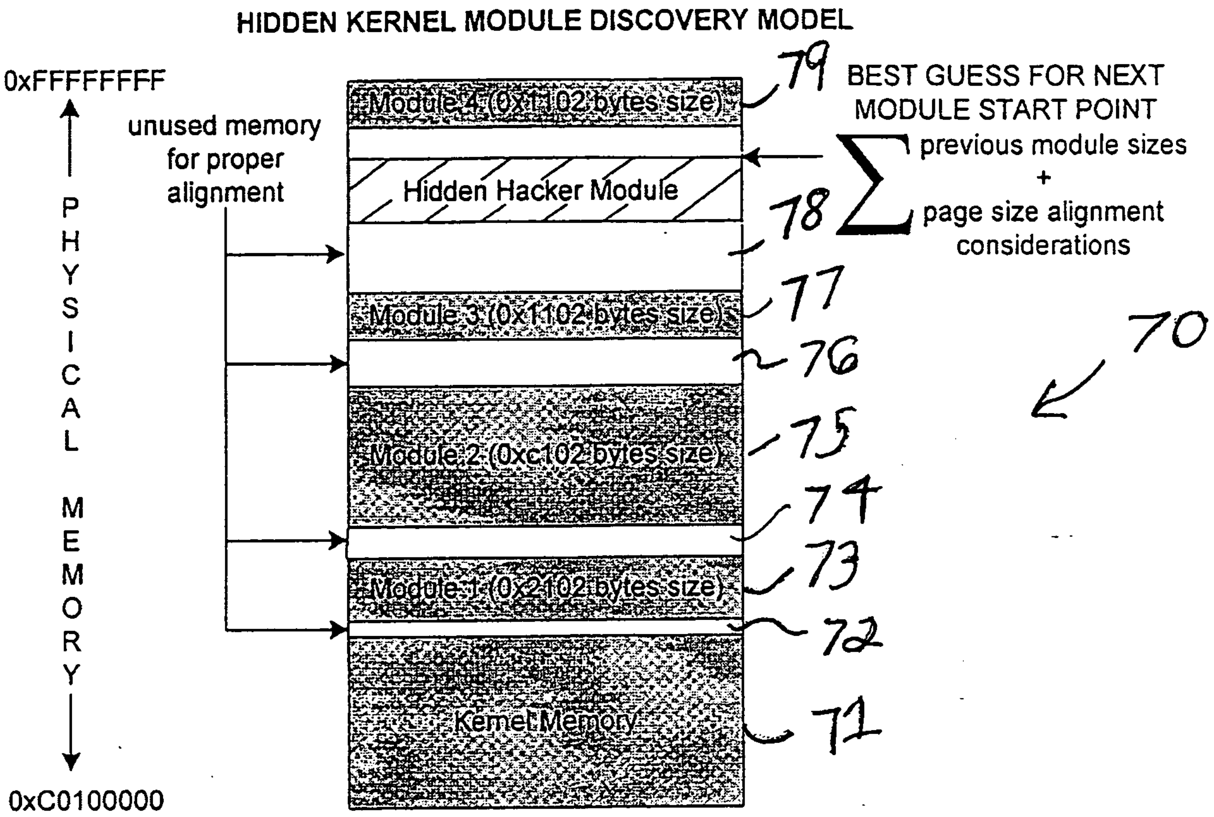
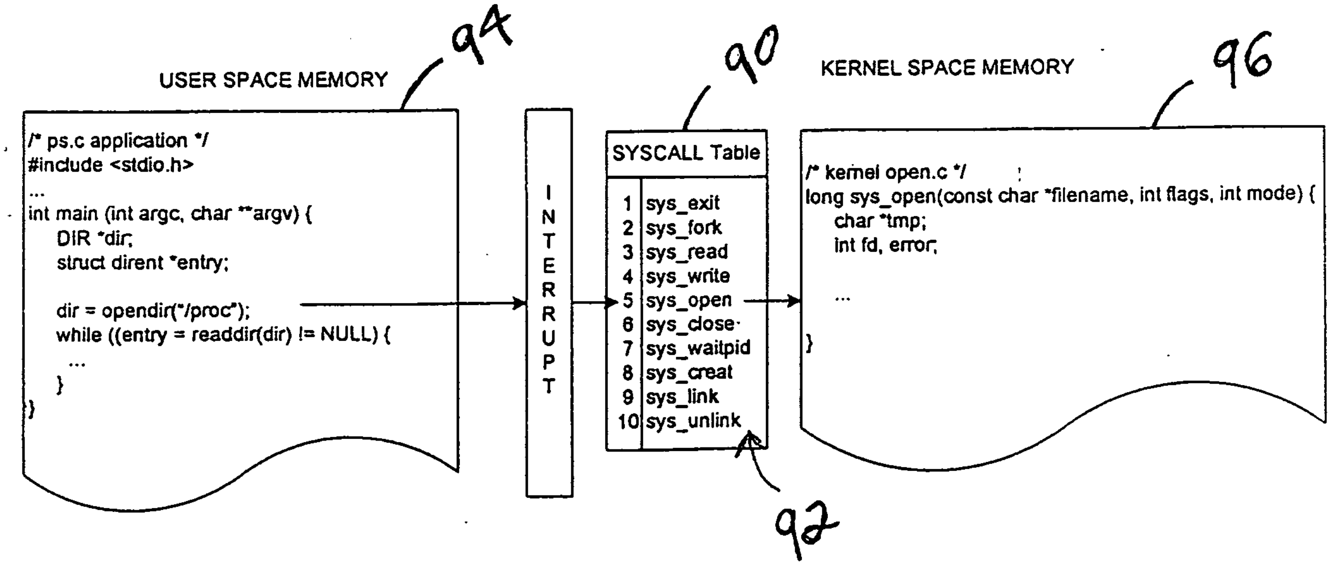

HIDDEN KERNEL MODULE DISCOVERY MODEL
0xFFFFFFFF
PHYSICAL MEMORY
0xC0100000
unused memory for proper alignment
Module 4 (0x1102 bytes size)
Hidden Hacker Module
Module 3 (0x1102 bytes size)
Module 2 (0xc102 bytes size)
Module 1 (0x2102 bytes size)
Kernel Memory
79
BEST GUESS FOR NEXT MODULE START POINT
∑ previous module sizes
+
page size alignment considerations
78
77
76
75
74
73
72
71
70

FIG. 7



```
/* ps.c application */
#include <stdio.h>
...
int main (int argc, char **argv) {
    DIR *dir;
    struct dirent *entry;

    dir = opendir("/proc");
    while ((entry = readdir(dir) != NULL) {
      ...
    }
}
```

SYSCALL Table	
1	sys_exit
2	sys_fork
3	sys_read
4	sys_write
5	sys_open
6	sys_close
7	sys_waitpid
8	sys_creat
9	sys_link
10	sys_unlink

```
/* kernel open.c */
long sys_open(const char *filename, int flags, int mode) {
    char *tmp;
    int fd, error;

    ...

}
```

FIG. 9

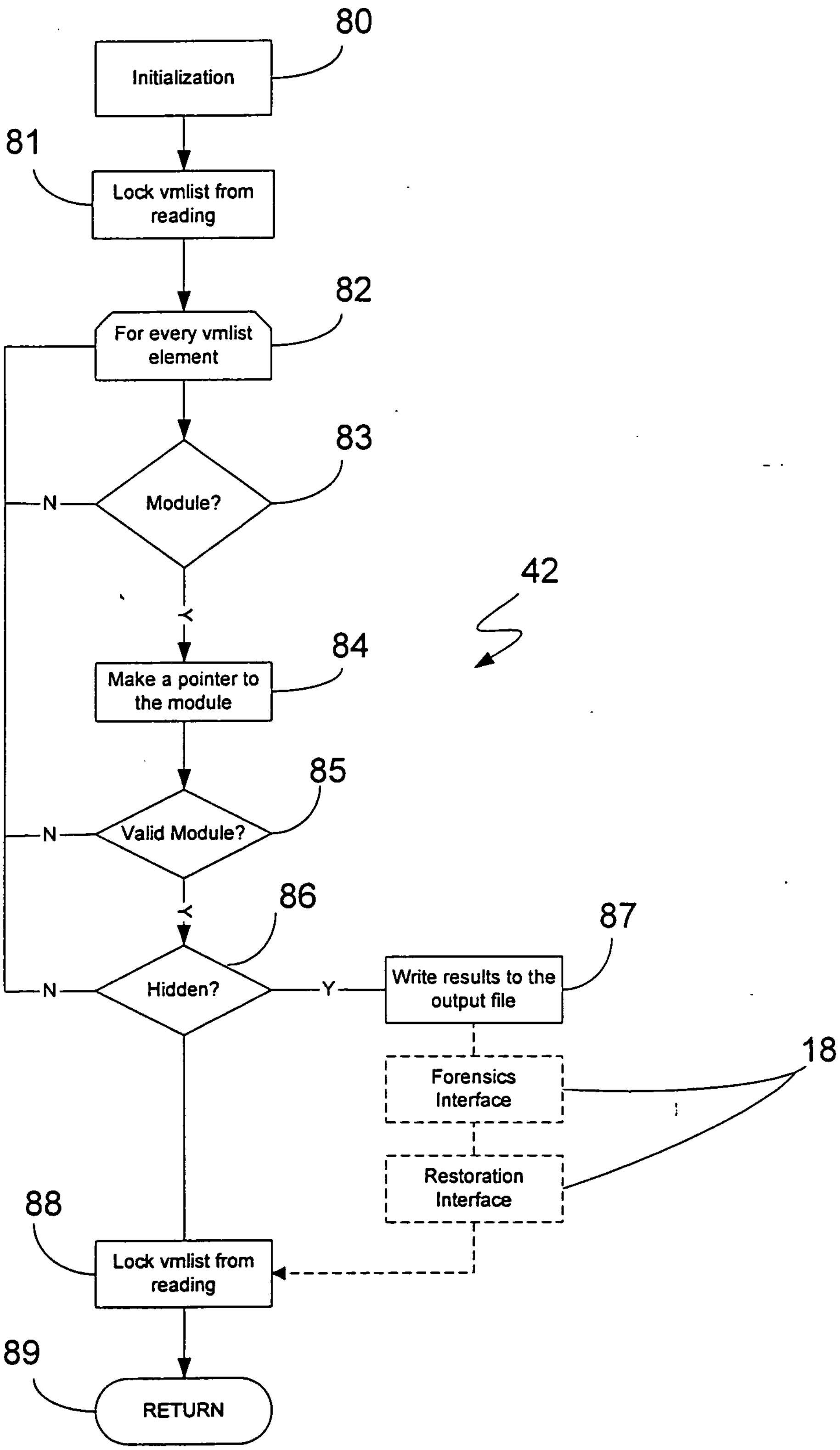

80
Initialization
81
Lock vmlist from reading
82
For every vmlist element
83
Module?
N
Y
84
Make a pointer to the module
85
Valid Module?
N
Y
86
Hidden?
N
Y
87
Write results to the output file
Forensics Interface
Restoration Interface
18
88
Lock vmlist from reading
89
RETURN
42

FIG. 8

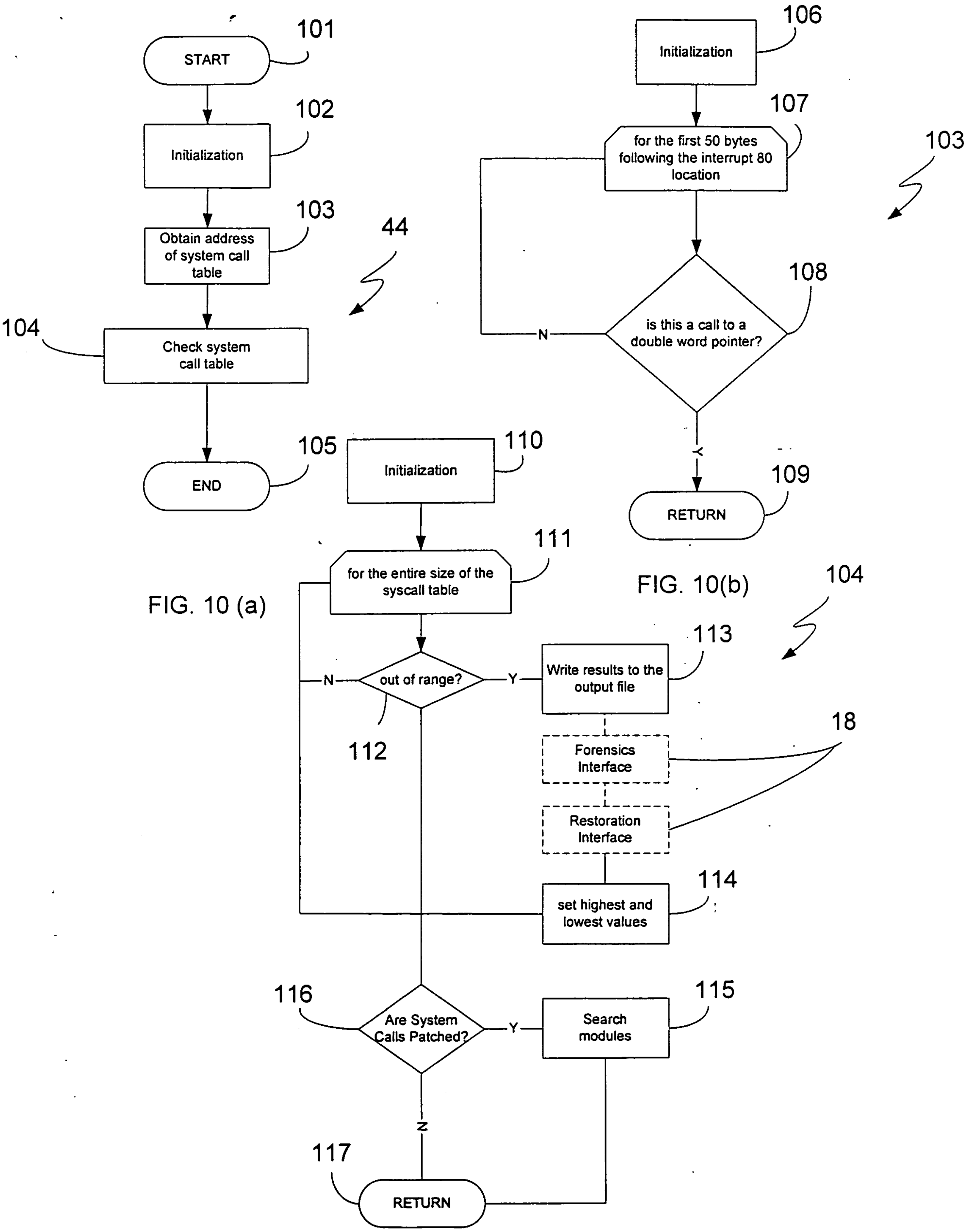

101
START
102
Initialization
103
Obtain address of system call table
44
104
Check system call table
105
END
106
Initialization
107
for the first 50 bytes following the interrupt 80 location
103
108
is this a call to a double word pointer?
N
Y
109
RETURN
110
Initialization
111
for the entire size of the syscall table
104
out of range?
N
Y
112
113
Write results to the output file
18
Forensics Interface
Restoration Interface
114
set highest and lowest values
116
Are System Calls Patched?
Y
115
Search modules
N
117
RETURN

FIG. 10 (a)

FIG. 10(b)

FIG. 10(c)

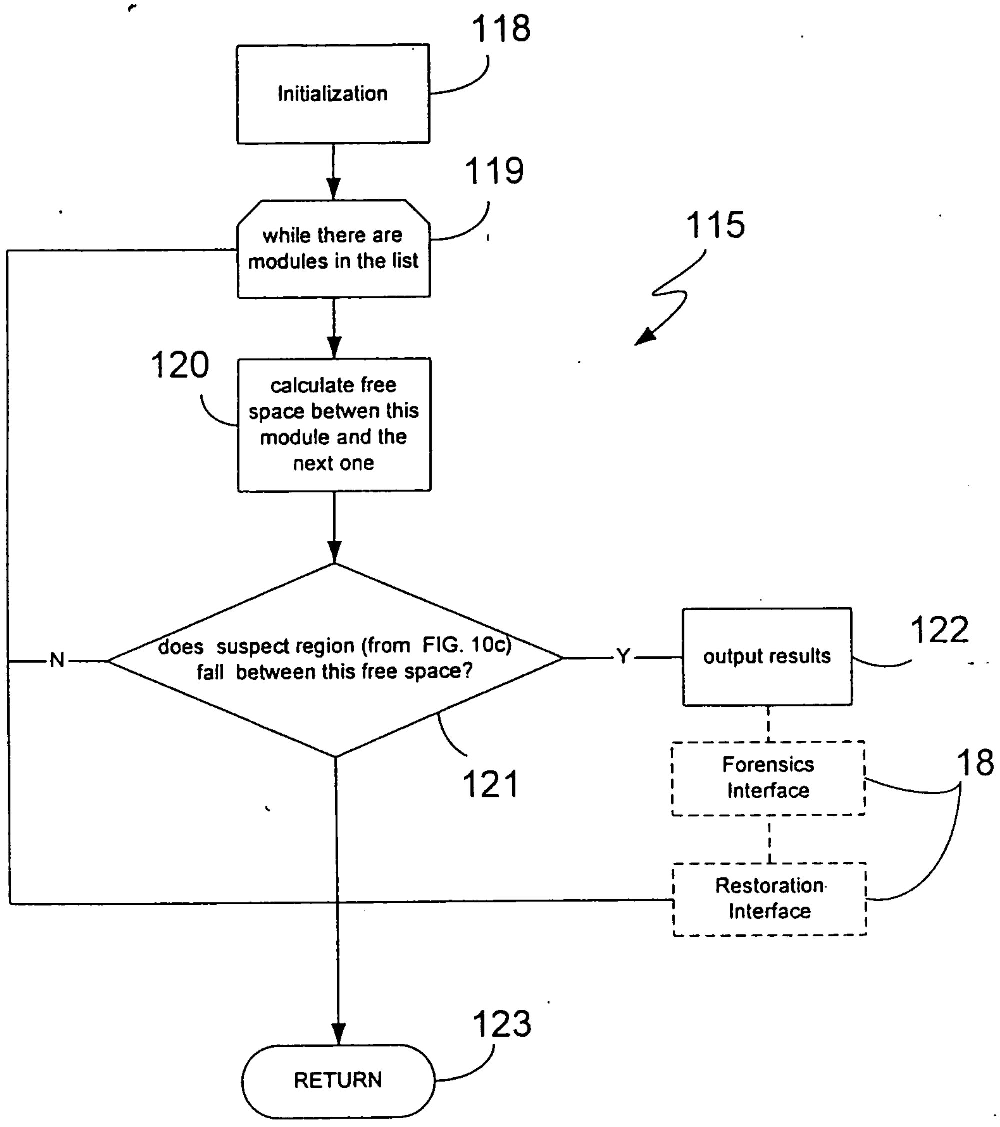
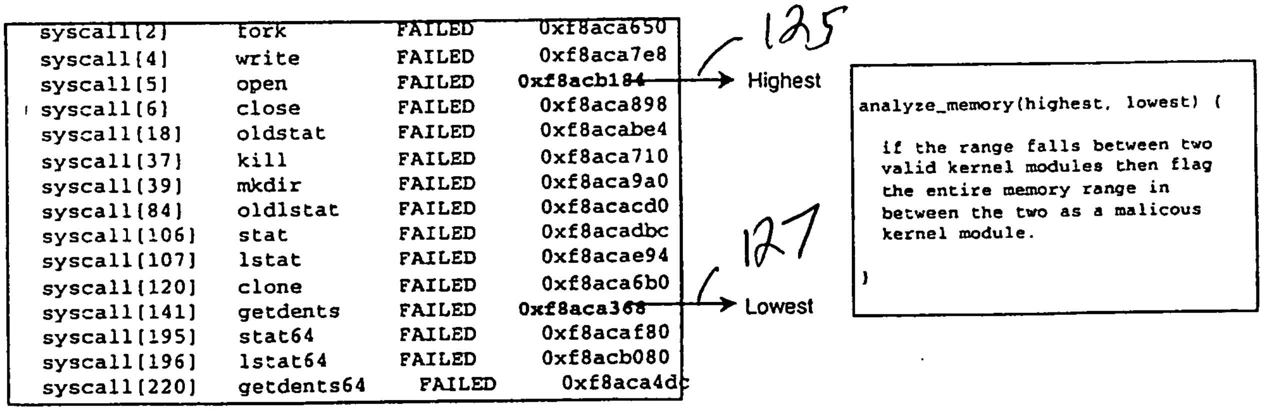

118
Initialization
119
while there are modules in the list
115
120
calculate free space betwen this module and the next one
does suspect region (from FIG. 10c) fall between this free space?
N
Y
121
output results
122
Forensics Interface
Restoration Interface
18
RETURN
123

FIG. 10(d)

IDENTIFIED SYSCALL ANOMALIES CAUSE BY ADORE v0.42



```
syscall[2]     fork          FAILED     0xf8aca650
syscall[4]     write         FAILED     0xf8aca7e8
syscall[5]     open          FAILED     0xf8acb184
syscall[6]     close         FAILED     0xf8aca898
syscall[18]    oldstat       FAILED     0xf8acabe4
syscall[37]    kill          FAILED     0xf8aca710
syscall[39]    mkdir         FAILED     0xf8aca9a0
syscall[84]    oldlstat      FAILED     0xf8acacd0
syscall[106]   stat          FAILED     0xf8acadbc
syscall[107]   lstat         FAILED     0xf8acae94
syscall[120]   clone         FAILED     0xf8aca6b0
syscall[141]   getdents      FAILED     0xf8aca368
syscall[195]   stat64        FAILED     0xf8acaf80
syscall[196]   lstat64       FAILED     0xf8acb080
syscall[220]   getdents64      FAILED     0xf8aca4dc
```

```
analyze_memory(highest, lowest) {

  if the range falls between two
  valid kernel modules then flag
  the entire memory range in
  between the two as a malicous
  kernel module.

}
```

FIG. 11

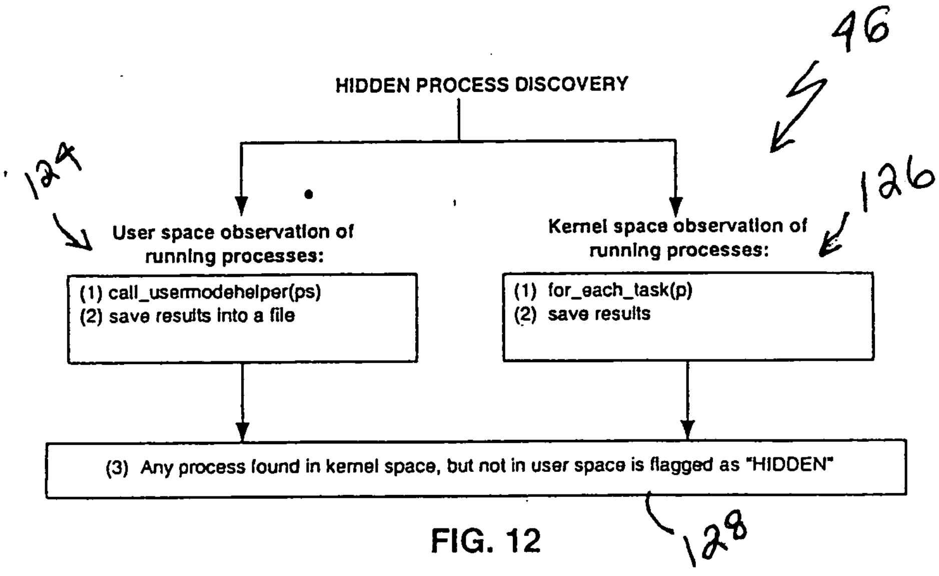

46
HIDDEN PROCESS DISCOVERY
124
User space observation of running processes:
(1) call_usermodehelper(ps)
(2) save results into a file
126
Kernel space observation of running processes:
(1) for_each_task(p)
(2) save results
(3) Any process found in kernel space, but not in user space is flagged as "HIDDEN"
128

FIG. 12

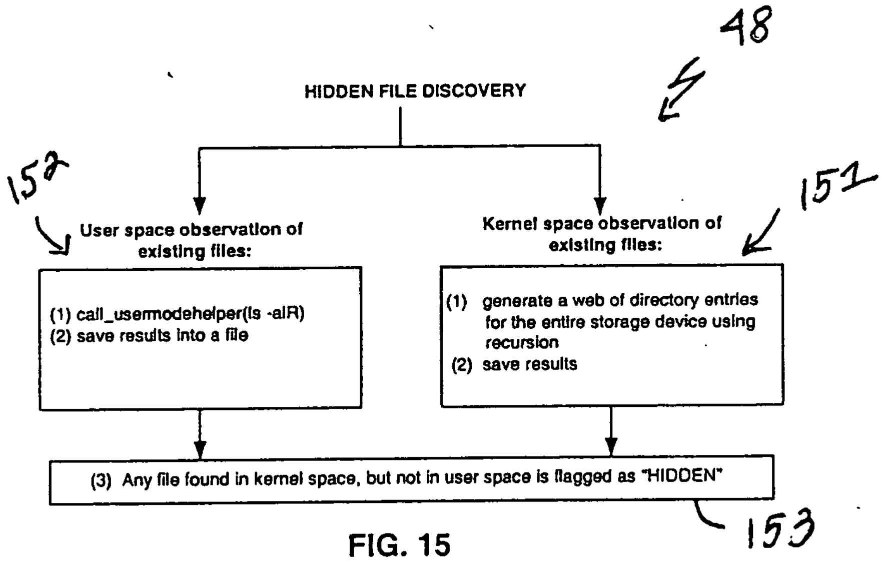

48
HIDDEN FILE DISCOVERY
152
User space observation of existing files:
(1) call_usermodehelper(ls -alR)
(2) save results into a file
151
Kernel space observation of existing files:
(1) generate a web of directory entries for the entire storage device using recursion
(2) save results
(3) Any file found in kernel space, but not in user space is flagged as "HIDDEN"
153

FIG. 15

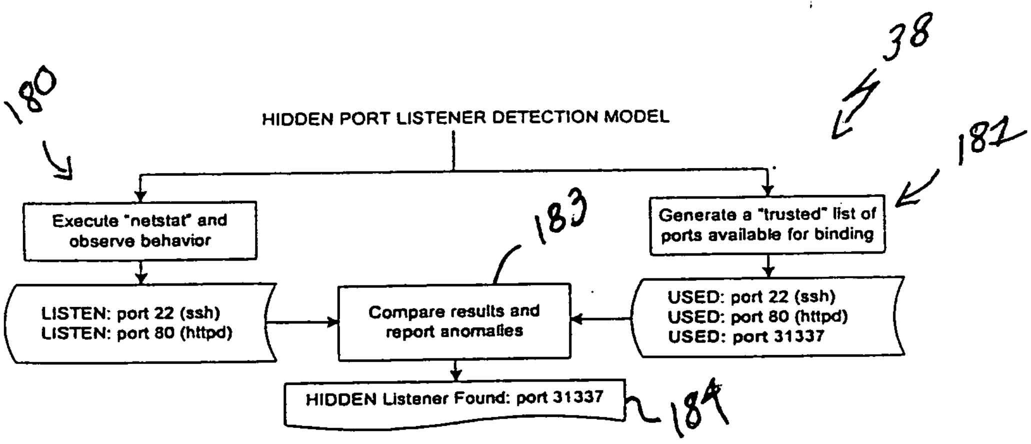

38
HIDDEN PORT LISTENER DETECTION MODEL
180
Execute "netstat" and observe behavior
LISTEN: port 22 (ssh)
LISTEN: port 80 (httpd)
183
Compare results and report anomalies
181
Generate a "trusted" list of ports available for binding
USED: port 22 (ssh)
USED: port 80 (httpd)
USED: port 31337
HIDDEN Listener Found: port 31337
184

FIG. 18

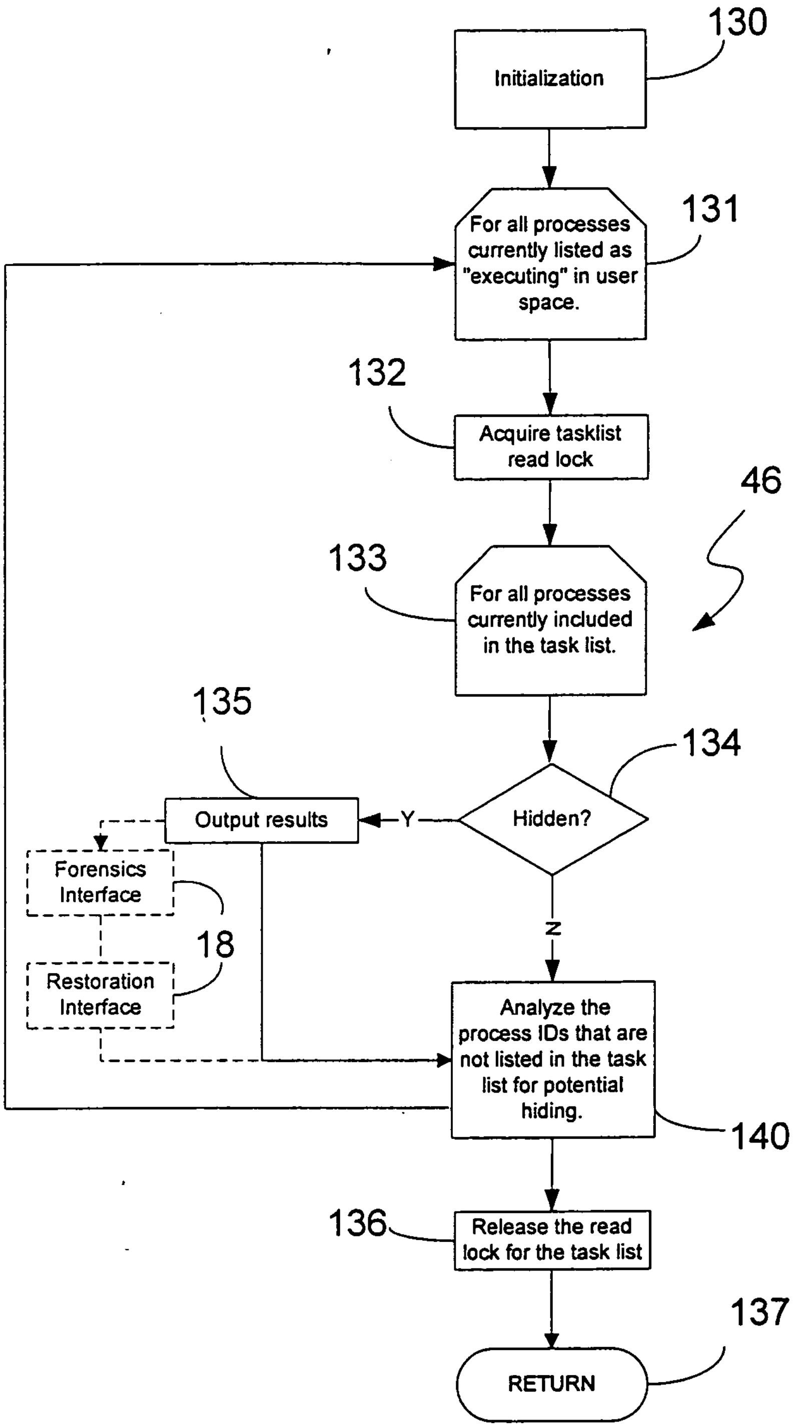

130
Initialization
131
For all processes currently listed as "executing" in user space.
132
Acquire tasklist read lock
46
133
For all processes currently included in the task list.
135
134
Output results
Y
Hidden?
Forensics Interface
18
Restoration Interface
N
Analyze the process IDs that are not listed in the task list for potential hiding.
140
136
Release the read lock for the task list
137
RETURN

FIG. 13

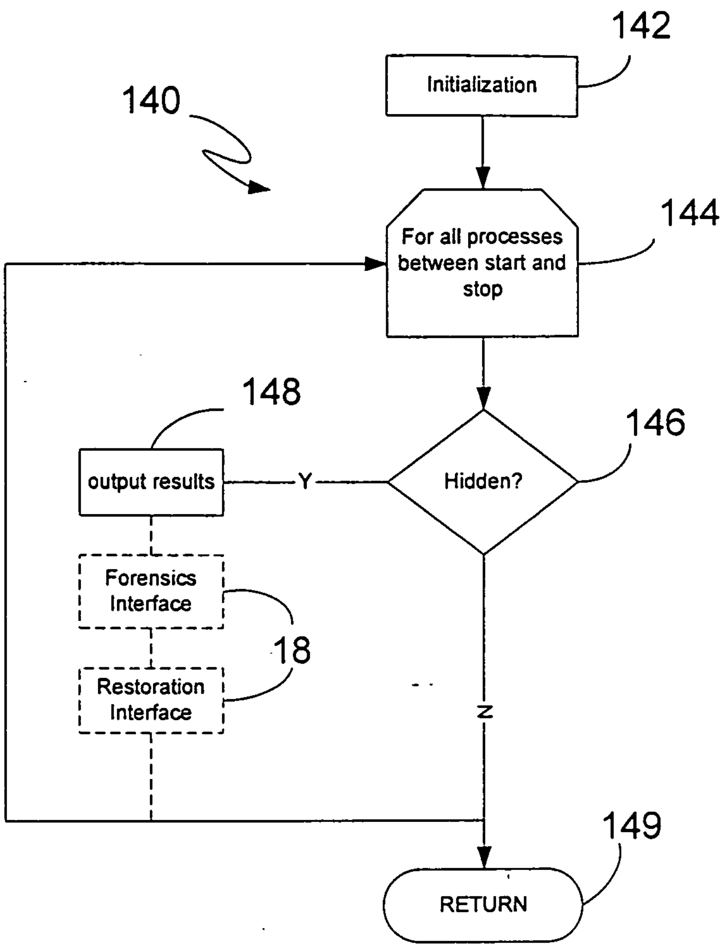


FIG. 14

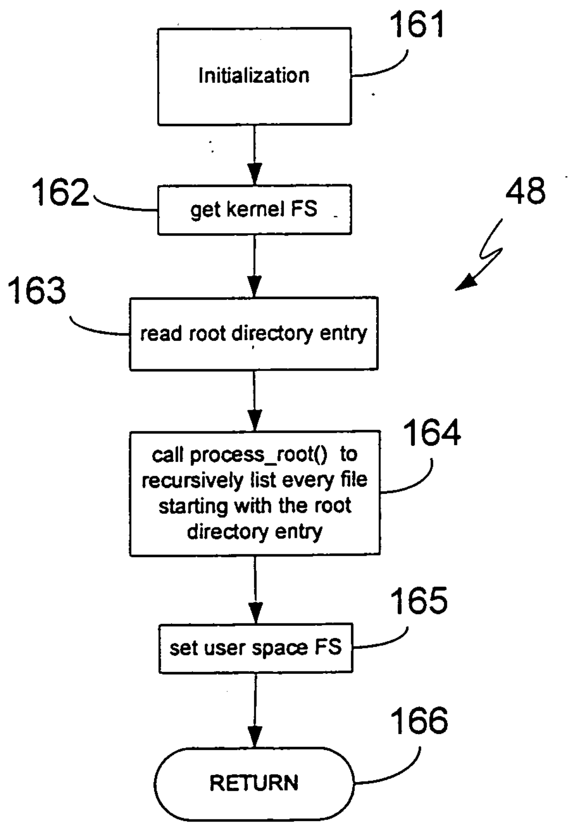

161
Initialization
162
get kernel FS
48
163
read root directory entry
164
call process_root() to recursively list every file starting with the root directory entry
165
set user space FS
166
RETURN

FIG. 16

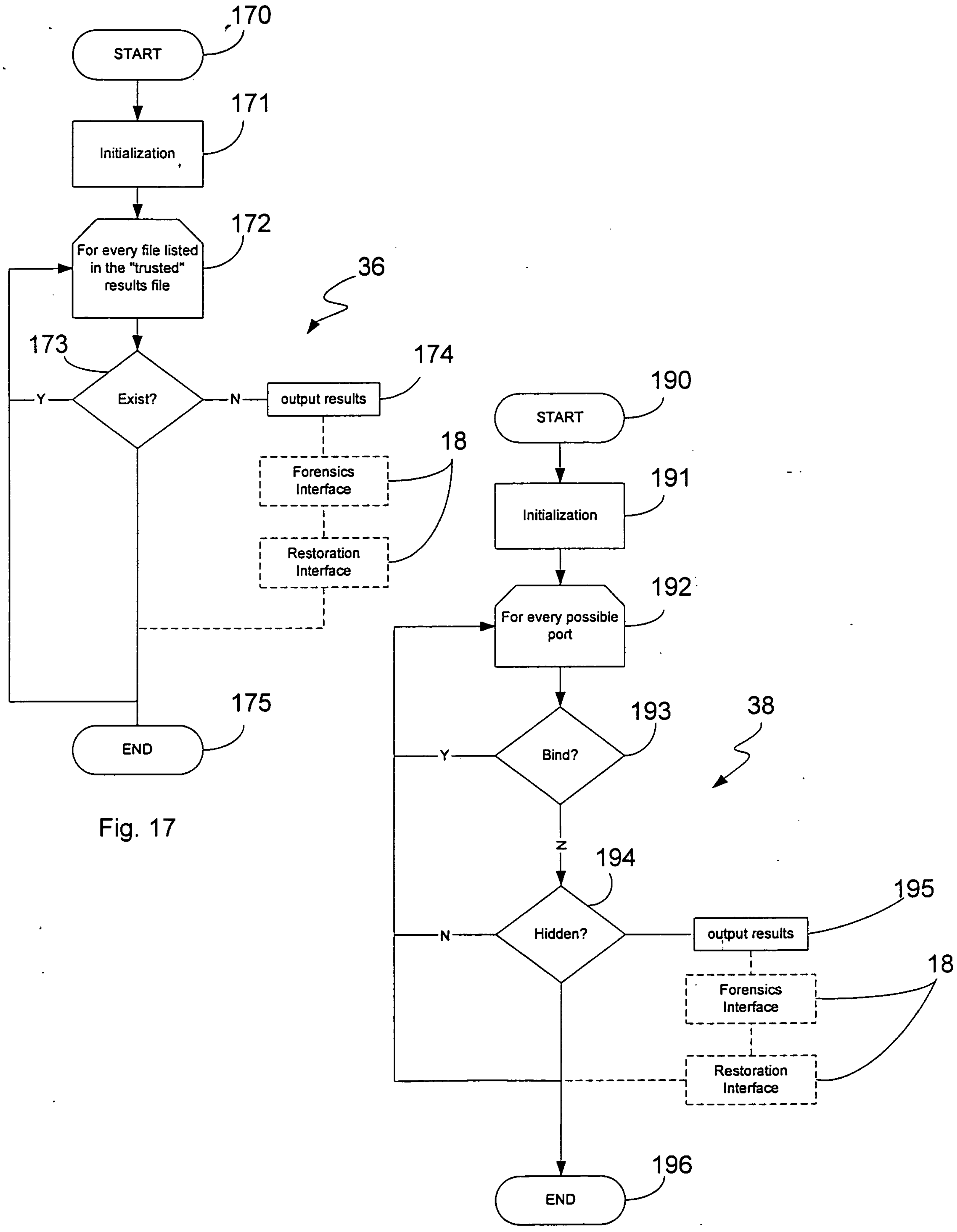
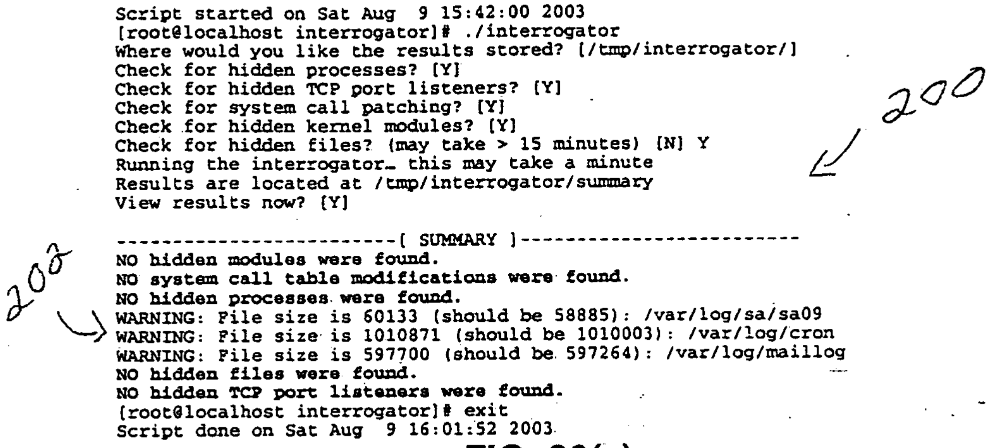

170
START
171
Initialization
172
For every file listed in the "trusted" results file
36
173
Exist?
Y
N
output results
174
Forensics Interface
Restoration Interface
18
175
END
190
START
191
Initialization
192
For every possible port
193
Bind?
Y
N
38
194
Hidden?
N
output results
195
Forensics Interface
Restoration Interface
18
196
END

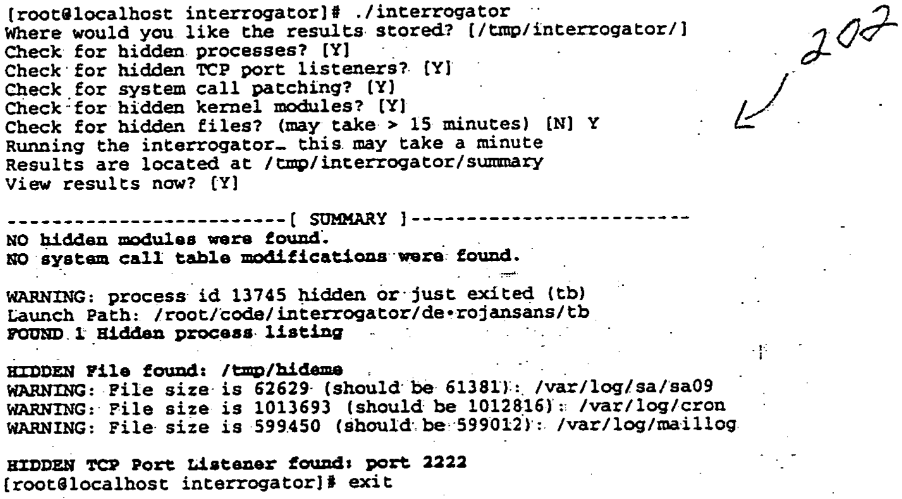
Fig. 17

FIG. 19



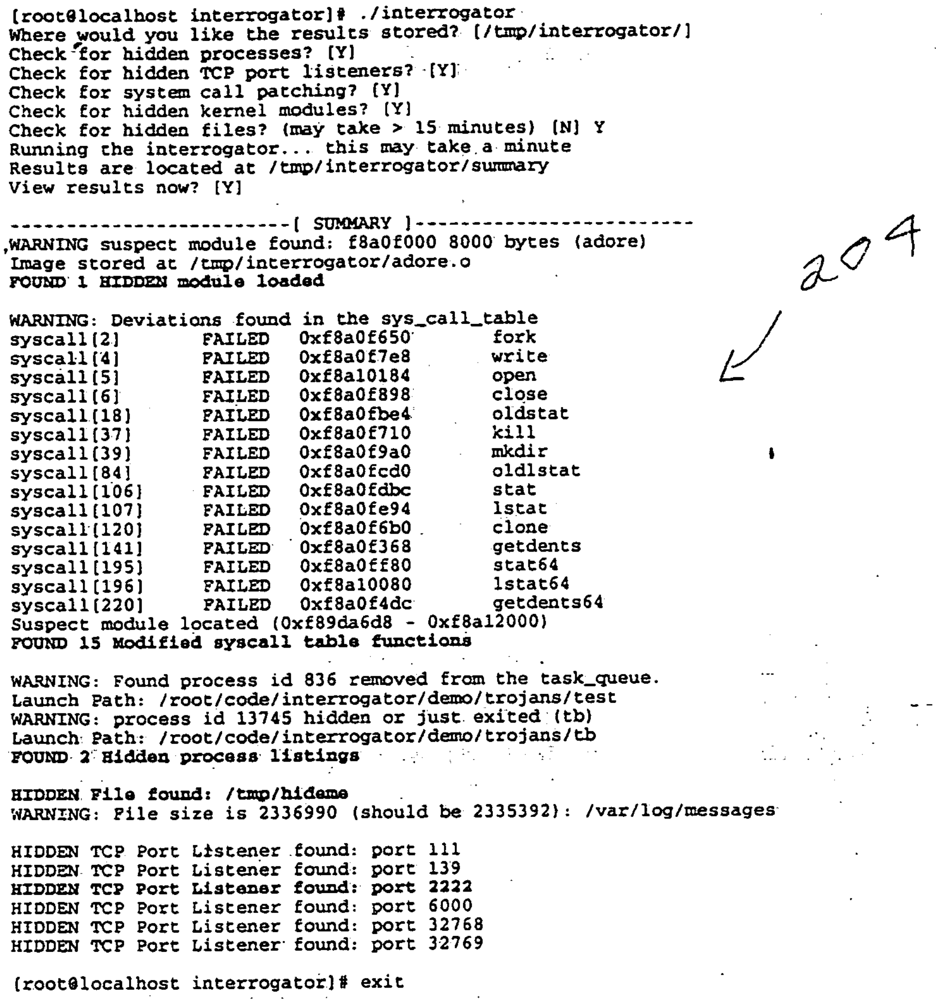
```
Script started on Sat Aug  9 15:42:00 2003
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator… this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
NO hidden modules were found.
NO system call table modifications were found.
NO hidden processes were found.
WARNING: File size is 60133 (should be 58885): /var/log/sa/sa09
WARNING: File size is 1010871 (should be 1010003): /var/log/cron
WARNING: File size is 597700 (should be 597264): /var/log/maillog
NO hidden files were found.
NO hidden TCP port listeners were found.
[root@localhost interrogator]# exit
Script done on Sat Aug  9 16:01:52 2003
```

FIG. 20(a)



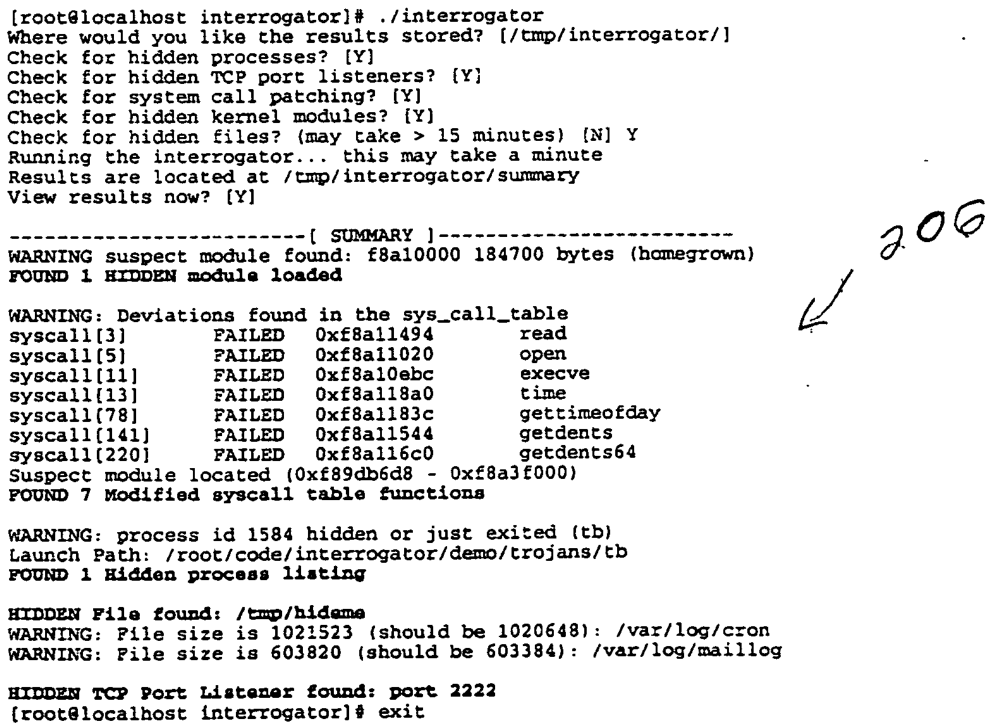
```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator… this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
NO hidden modules were found.
NO system call table modifications were found.

WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/de•rojansans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 62629 (should be 61381): /var/log/sa/sa09
WARNING: File size is 1013693 (should be 1012816): /var/log/cron
WARNING: File size is 599450 (should be 599012): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

FIG. 20(b)



```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: f8a0f000 8000 bytes (adore)
Image stored at /tmp/interrogator/adore.o
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]        FAILED   0xf8a0f650       fork
syscall[4]        FAILED   0xf8a0f7e8       write
syscall[5]        FAILED   0xf8a10184       open
syscall[6]        FAILED   0xf8a0f898       close
syscall[18]       FAILED   0xf8a0fbe4       oldstat
syscall[37]       FAILED   0xf8a0f710       kill
syscall[39]       FAILED   0xf8a0f9a0       mkdir
syscall[84]       FAILED   0xf8a0fcd0       oldlstat
syscall[106]      FAILED   0xf8a0fdbc       stat
syscall[107]      FAILED   0xf8a0fe94       lstat
syscall[120]      FAILED   0xf8a0f6b0       clone
syscall[141]      FAILED   0xf8a0f368       getdents
syscall[195]      FAILED   0xf8a0ff80       stat64
syscall[196]      FAILED   0xf8a10080       lstat64
syscall[220]      FAILED   0xf8a0f4dc       getdents64
Suspect module located (0xf89da6d8 - 0xf8a12000)
FOUND 15 Modified syscall table functions

WARNING: Found process id 836 removed from the task_queue.
Launch Path: /root/code/interrogator/demo/trojans/test
WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 2 Hidden process listings

HIDDEN File found: /tmp/hideme
WARNING: File size is 2336990 (should be 2335392): /var/log/messages

HIDDEN TCP Port Listener found: port 111
HIDDEN TCP Port Listener found: port 139
HIDDEN TCP Port Listener found: port 2222
HIDDEN TCP Port Listener found: port 6000
HIDDEN TCP Port Listener found: port 32768
HIDDEN TCP Port Listener found: port 32769

[root@localhost interrogator]# exit
```

FIG. 20(c)



```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: f8a10000 184700 bytes (homegrown)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[3]        FAILED   0xf8a11494       read
syscall[5]        FAILED   0xf8a11020       open
syscall[11]       FAILED   0xf8a10ebc       execve
syscall[13]       FAILED   0xf8a118a0       time
syscall[78]       FAILED   0xf8a1183c       gettimeofday
syscall[141]      FAILED   0xf8a11544       getdents
syscall[220]      FAILED   0xf8a116c0       getdents64
Suspect module located (0xf89db6d8 - 0xf8a3f000)
FOUND 7 Modified syscall table functions

WARNING: process id 1584 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 1021523 (should be 1020648): /var/log/cron
WARNING: File size is 603820 (should be 603384): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

FIG. 20(d)

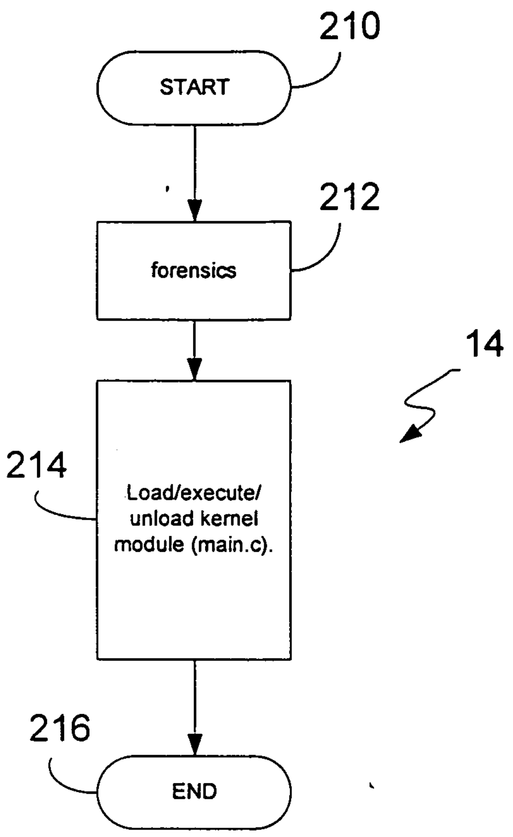


FIG. 21

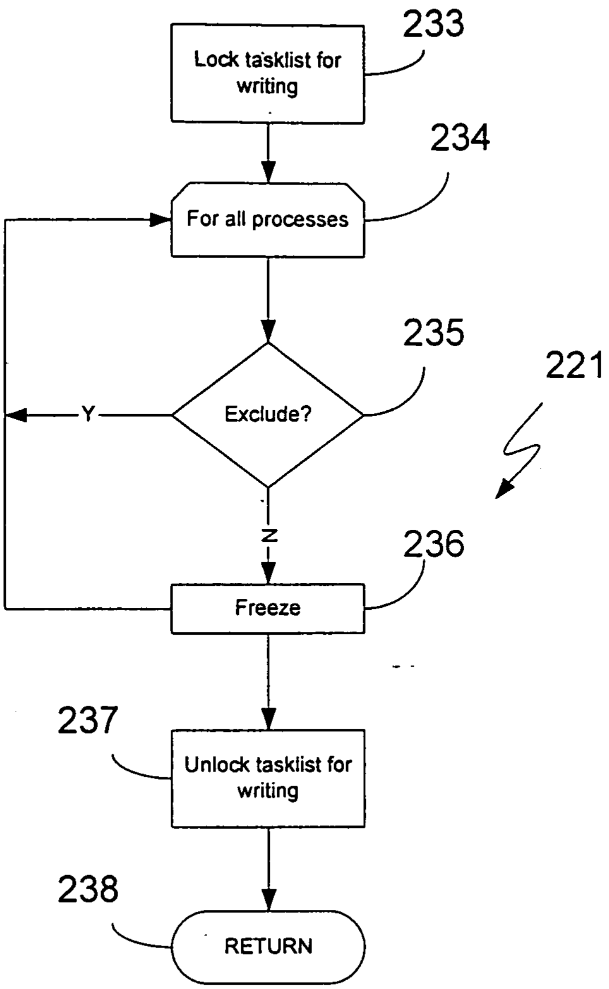


FIG. 23

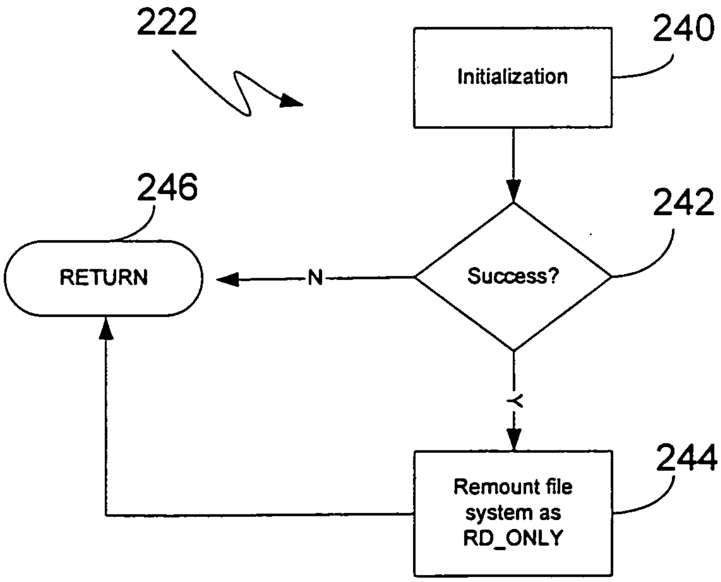


FIG. 24

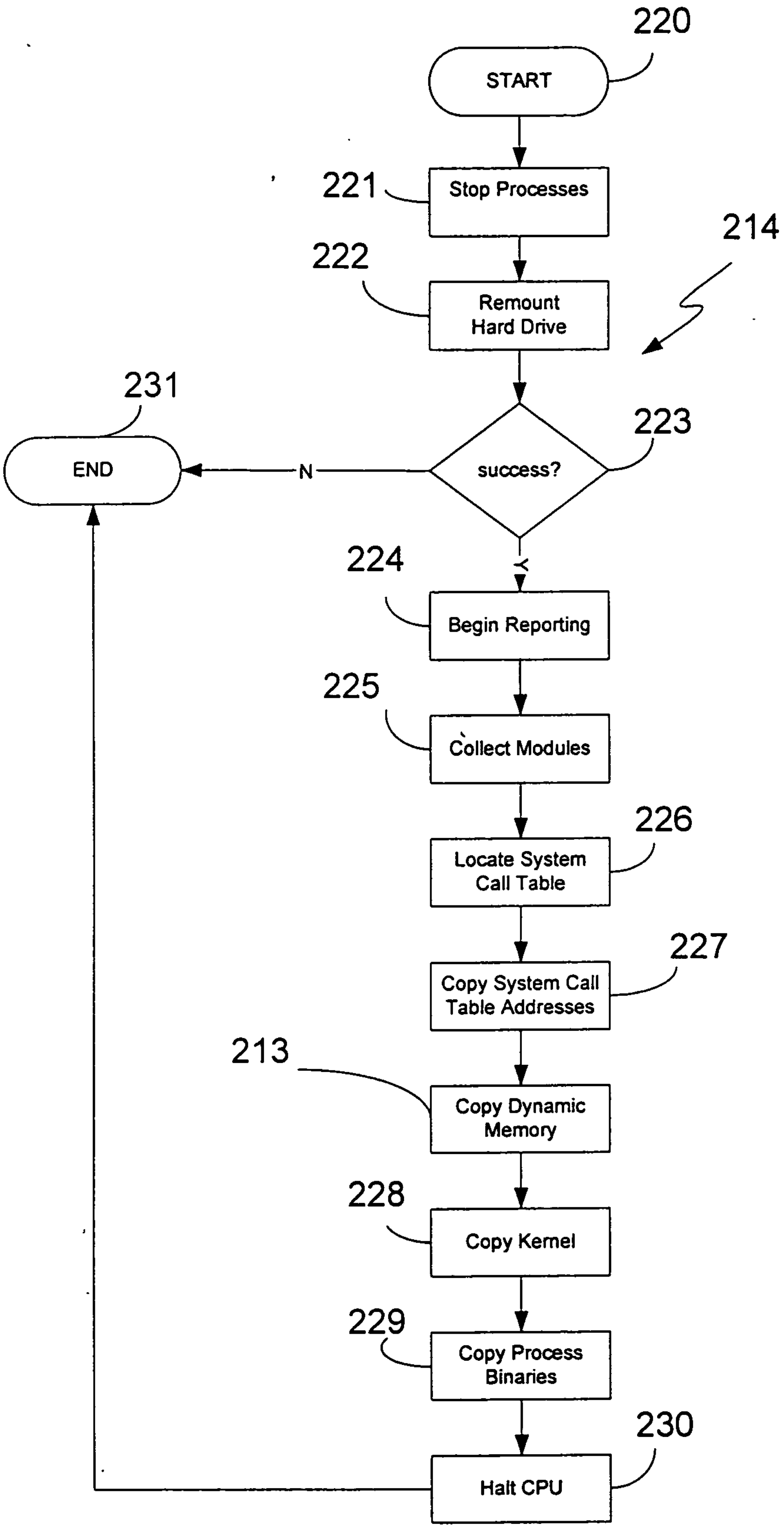


FIG. 22(a)

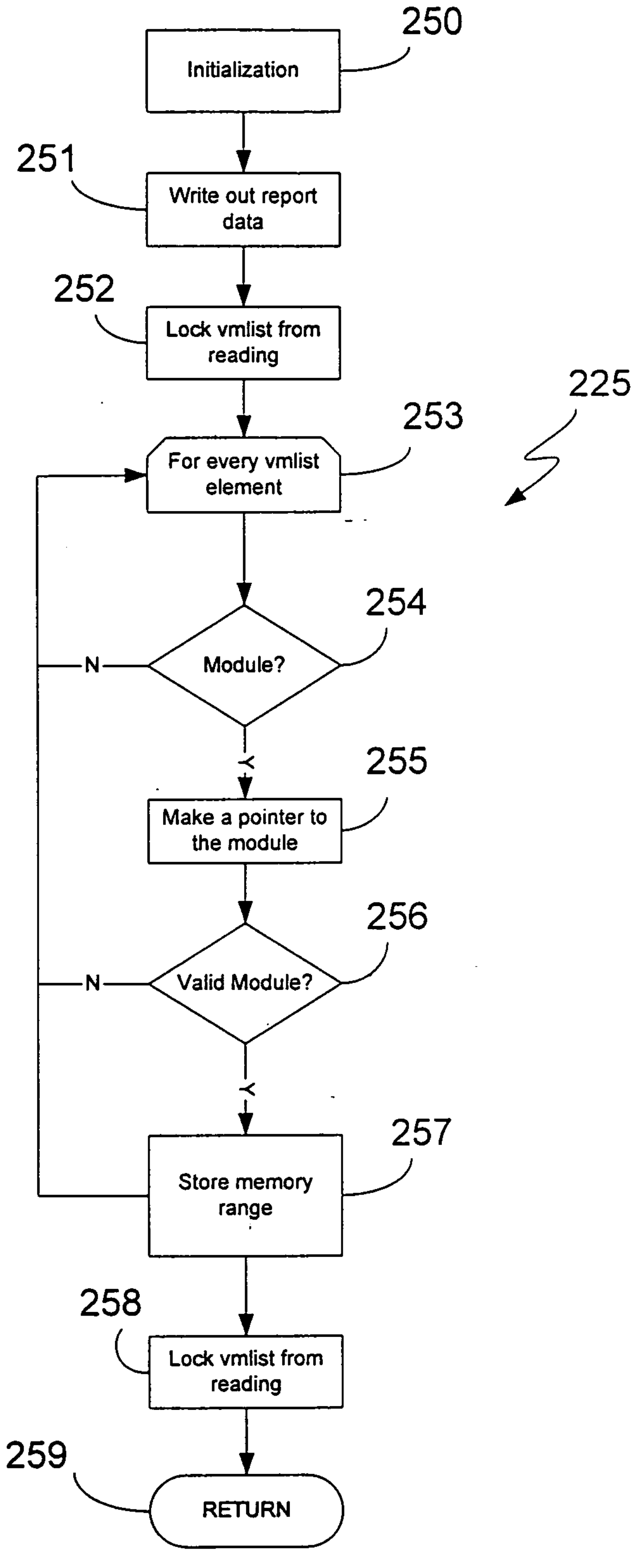


FIG. 25(a)

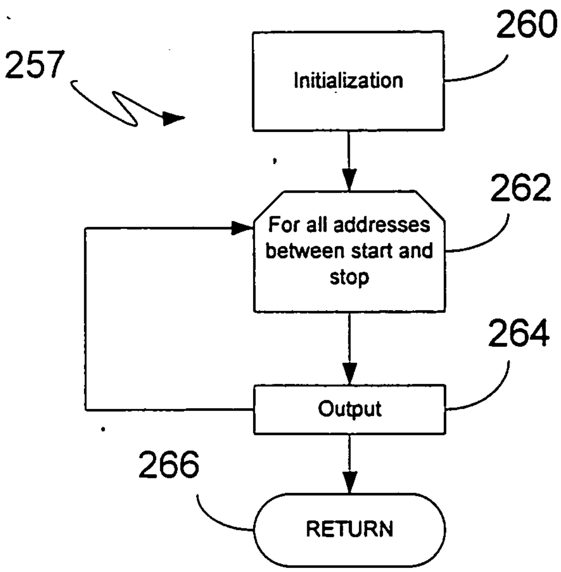


FIG. 26

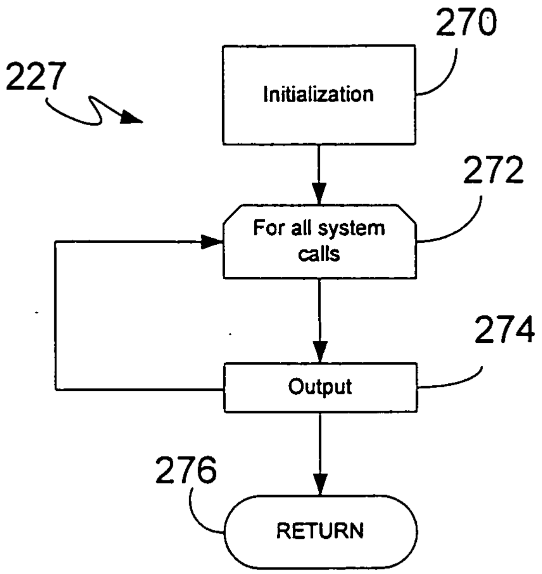


FIG. 27(a)

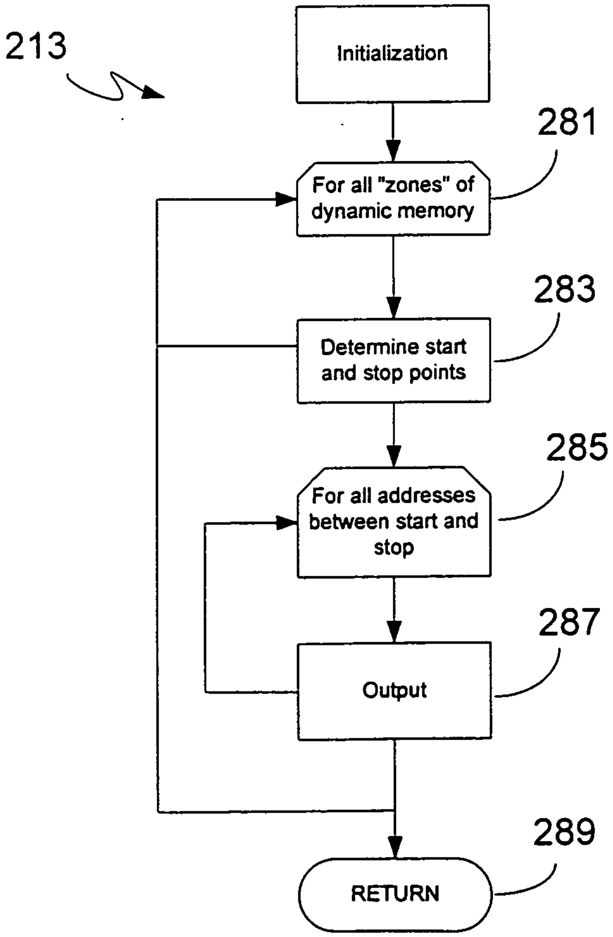

213
Initialization
For all "zones" of dynamic memory
281
Determine start and stop points
283
For all addresses between start and stop
285
Output
287
RETURN
289

FIG. 28(a)

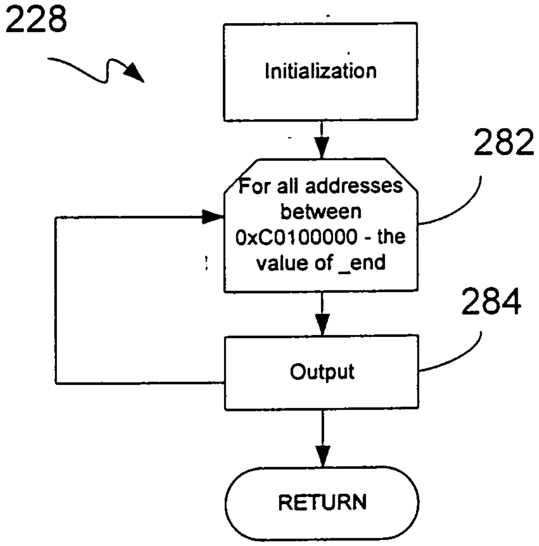
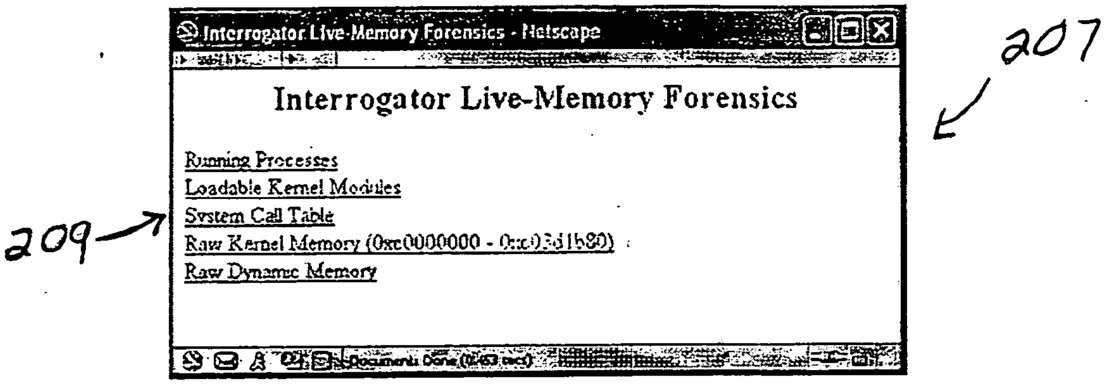


FIG. 28(c)



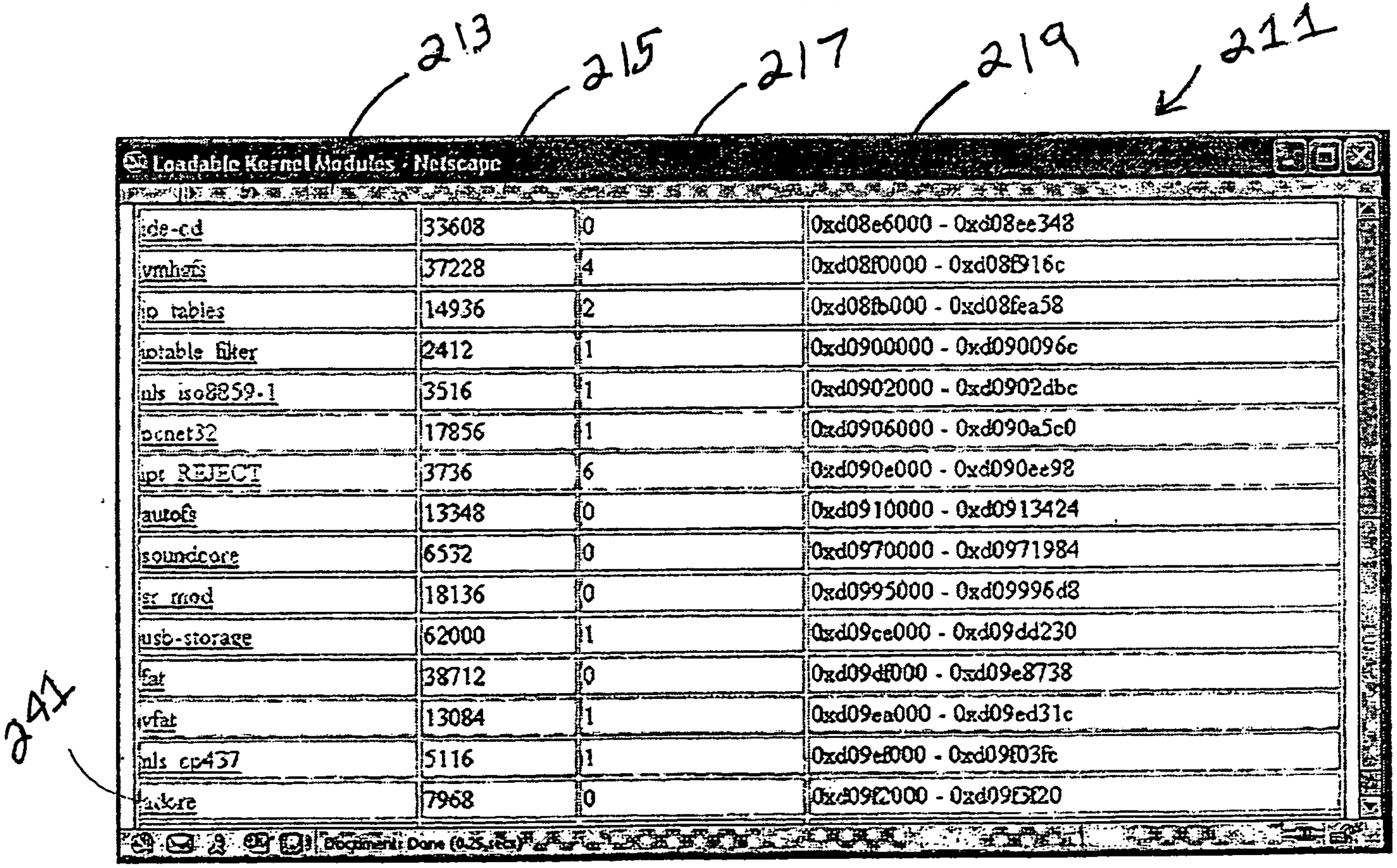
Interrogator Live-Memory Forensics - Netscape

Interrogator Live-Memory Forensics

Running Processes
Loadable Kernel Modules
System Call Table
Raw Kernel Memory (0xc0000000 - 0xc03d1b80)
Raw Dynamic Memory

Document: Done (0.63 secs)

FIG. 22(b)

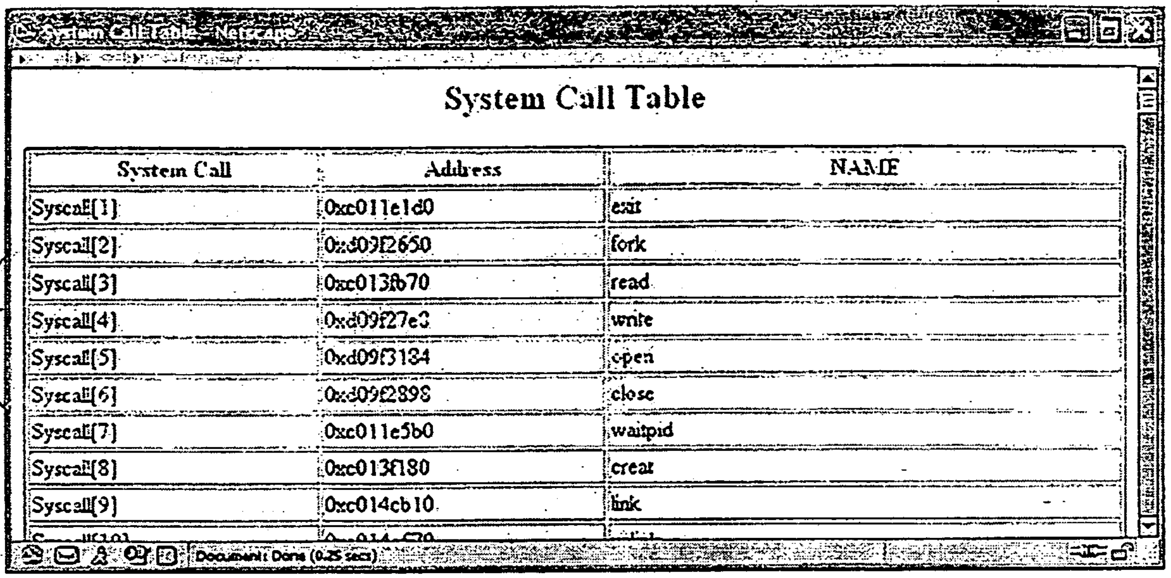


Loadable Kernel Modules - Netscape

ide-cd	33608	0	0xd08e6000 - 0xd08ee348
vmhgfs	37228	4	0xd08f0000 - 0xd08f916c
ip_tables	14936	2	0xd08fb000 - 0xd08fea58
iptable_filter	2412	1	0xd0900000 - 0xd090096c
nls_iso8859-1	3516	1	0xd0902000 - 0xd0902dbc
pcnet32	17856	1	0xd0906000 - 0xd090a5c0
ipt_REJECT	3736	6	0xd090e000 - 0xd090ee98
autofs	13348	0	0xd0910000 - 0xd0913424
soundcore	6532	0	0xd0970000 - 0xd0971984
sr_mod	18136	0	0xd0995000 - 0xd09996d8
usb-storage	62000	1	0xd09ce000 - 0xd09dd230
fat	38712	0	0xd09df000 - 0xd09e8738
vfat	13084	1	0xd09ea000 - 0xd09ed31c
nls_cp437	5116	1	0xd09ef000 - 0xd09f03fc
adore	7968	0	0xd09f2000 - 0xd09f3f20

Document: Done (0.25 secs)

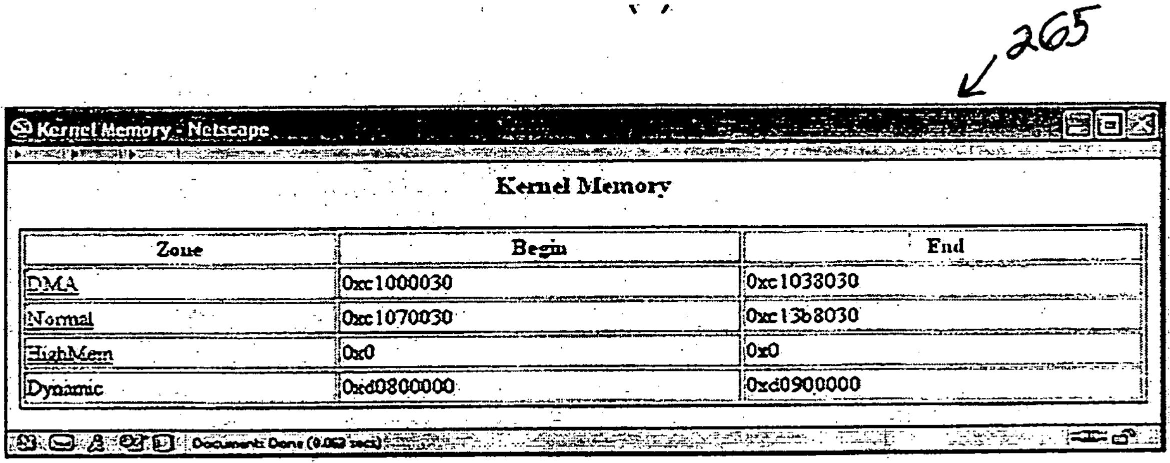
FIG. 25(b)



System Call Table

System Call	Address	NAME
Syscall[1]	0xc011e1d0	exit
Syscall[2]	0xd09f2650	fork
Syscall[3]	0xc013fb70	read
Syscall[4]	0xd09f27e3	write
Syscall[5]	0xd09f3134	open
Syscall[6]	0xd09f2898	close
Syscall[7]	0xc011e5b0	waitpid
Syscall[8]	0xc013f180	creat
Syscall[9]	0xc014cb10	link

FIG. 27(b)



Kernel Memory

Zone	Begin	End
DMA	0xc1000030	0xc1038030
Normal	0xc1070030	0xc13b8030
HighMem	0x0	0x0
Dynamic	0xd0800000	0xd0900000

FIG. 28(b)

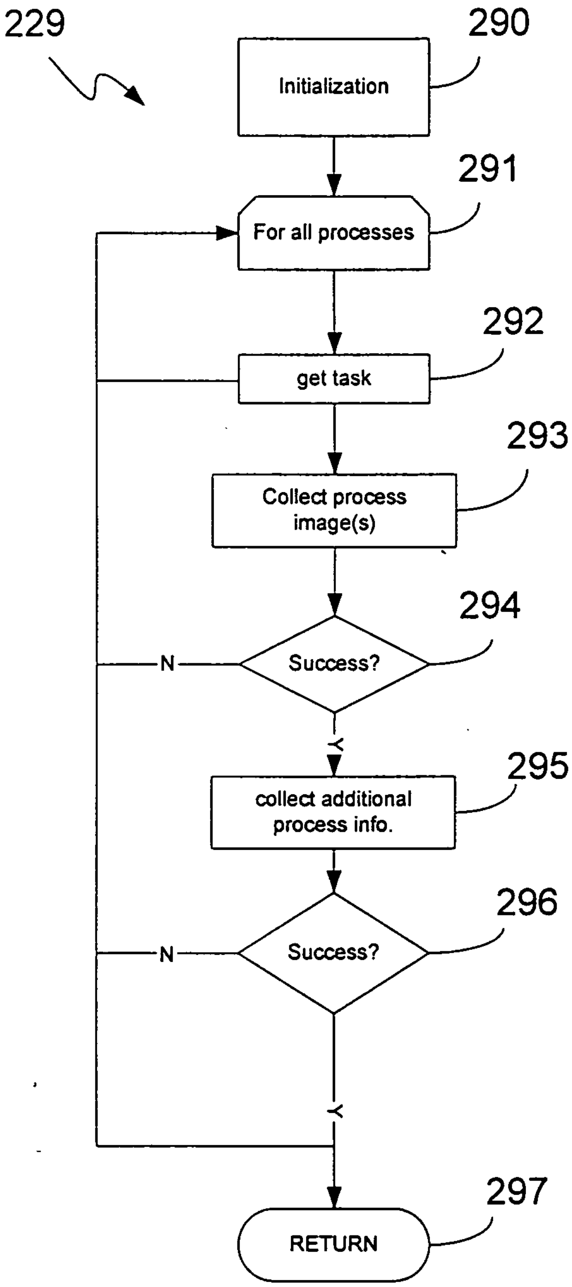


FIG. 29(a)

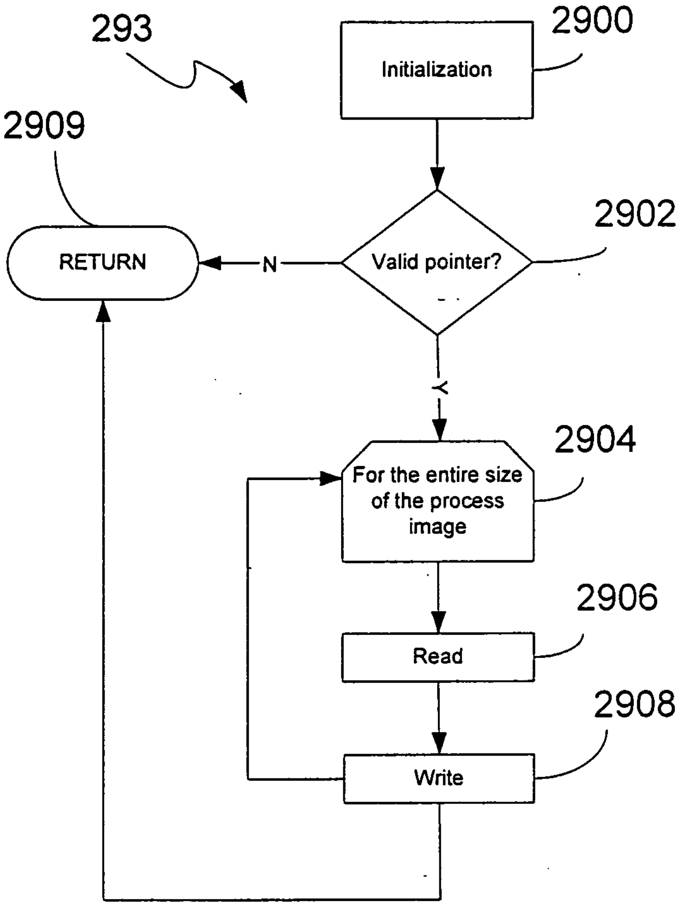


FIG. 29(b)

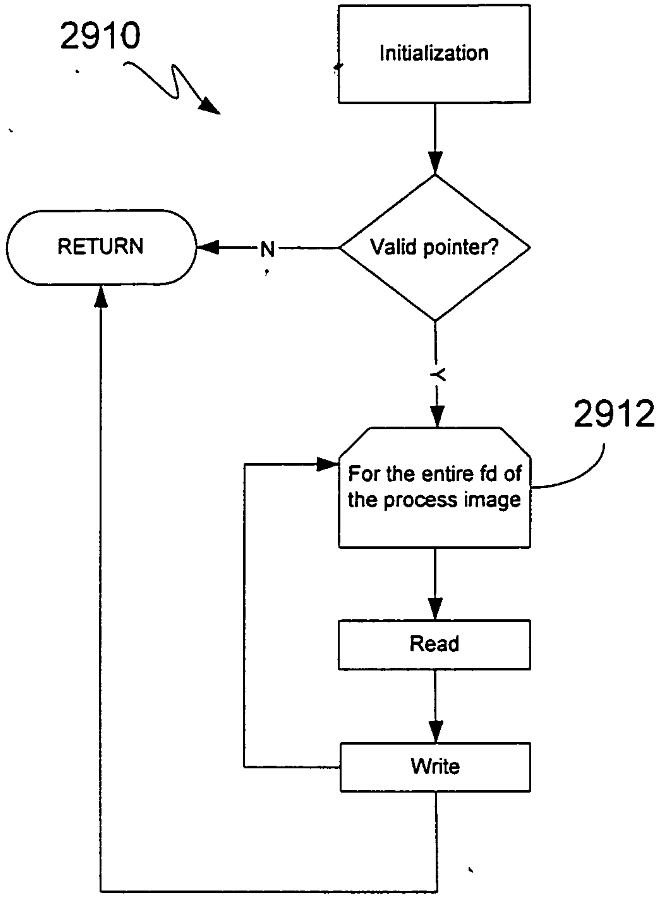


FIG. 29(c)

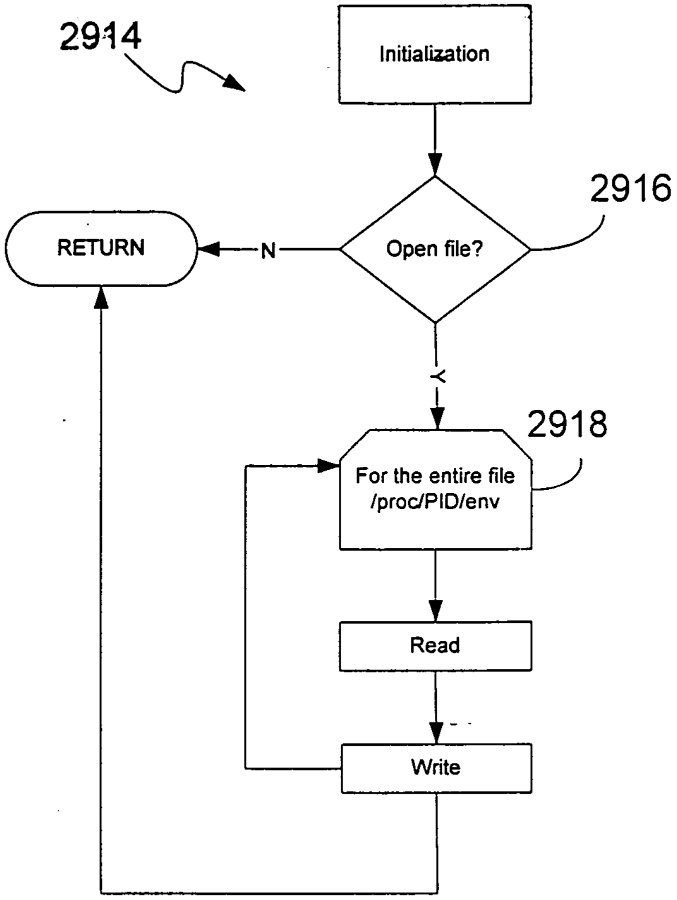


FIG. 29(d)

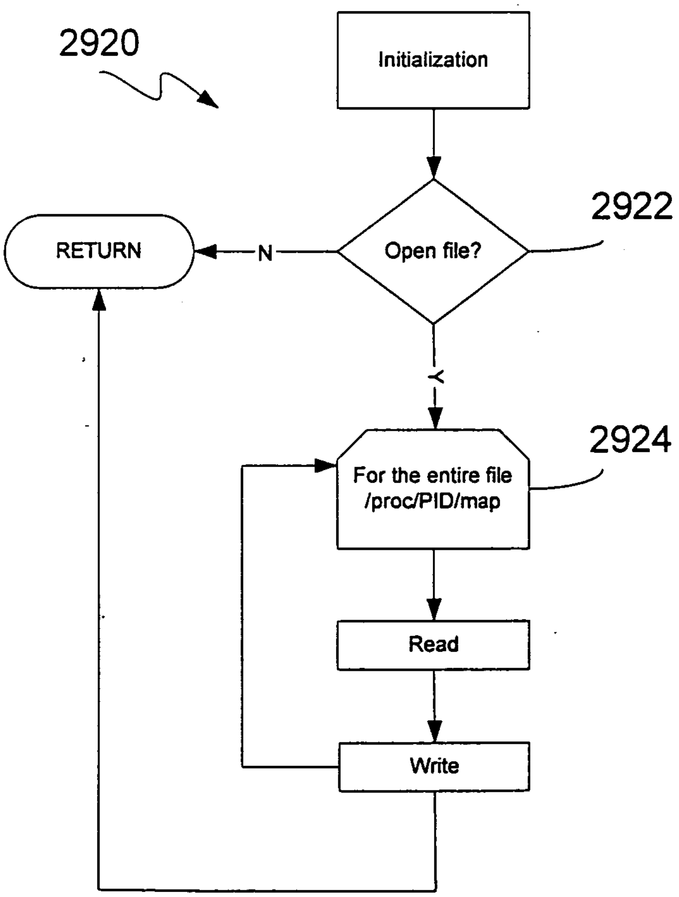


FIG. 29(e)

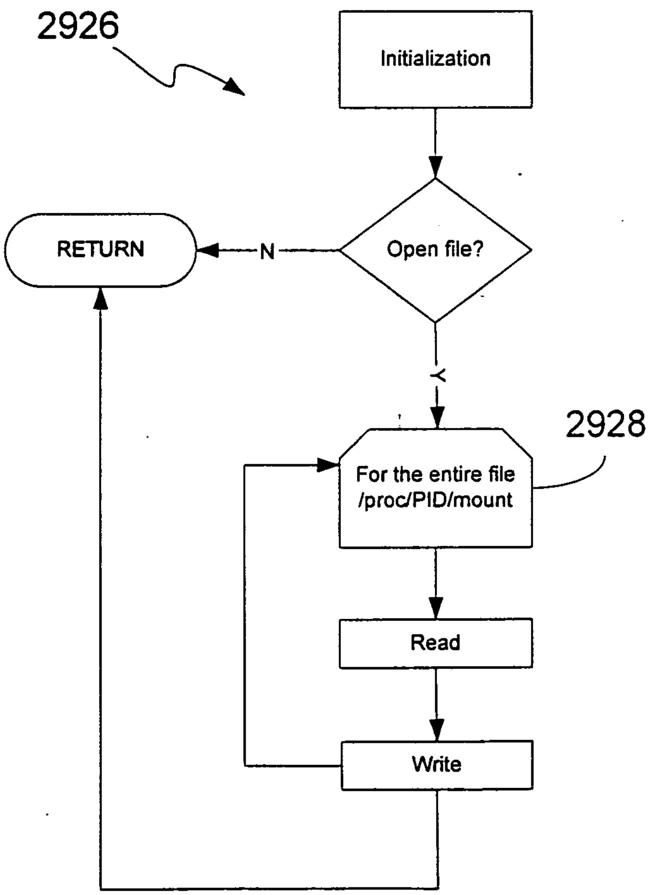


FIG. 29(f)

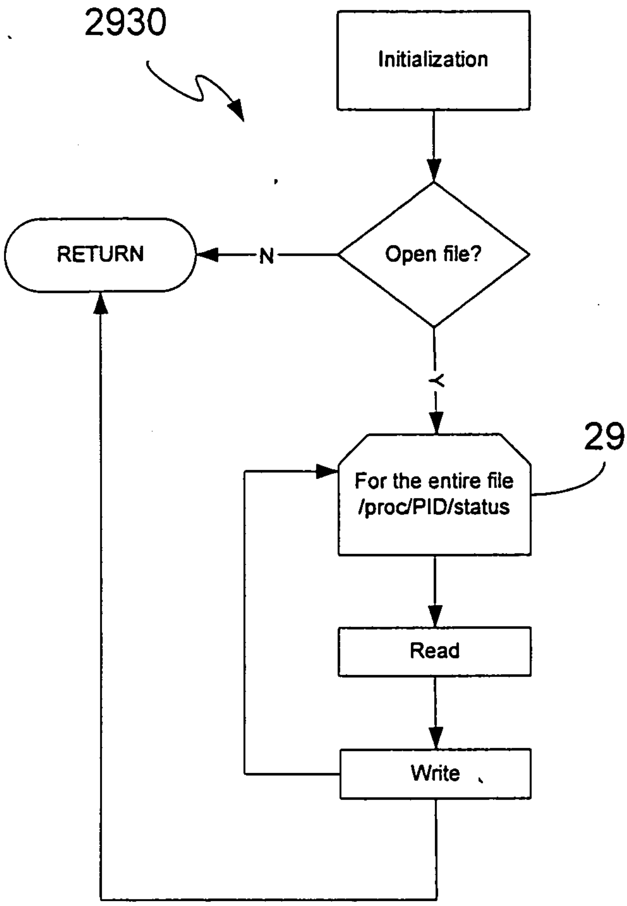


FIG. 29(g)

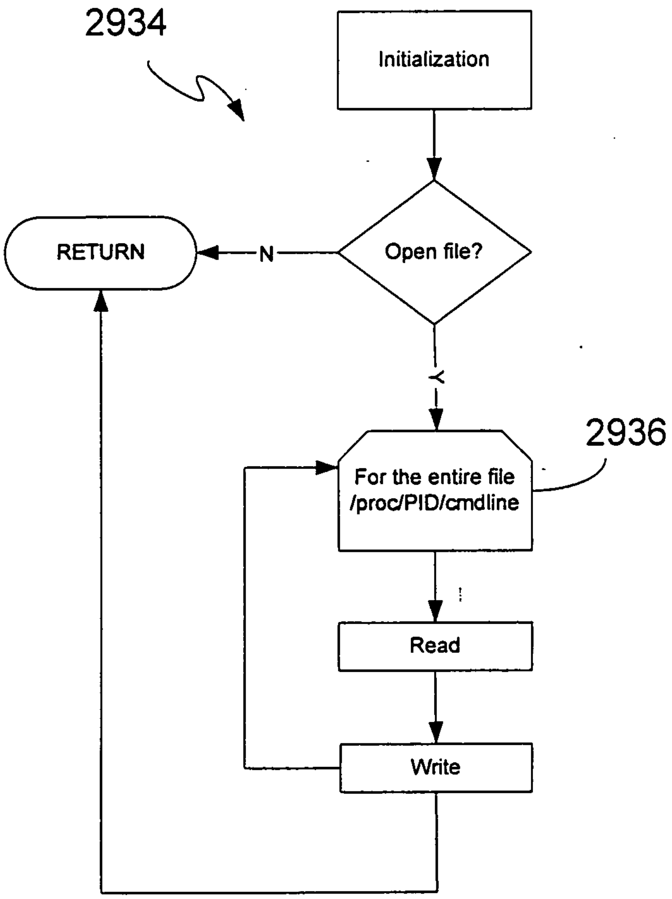
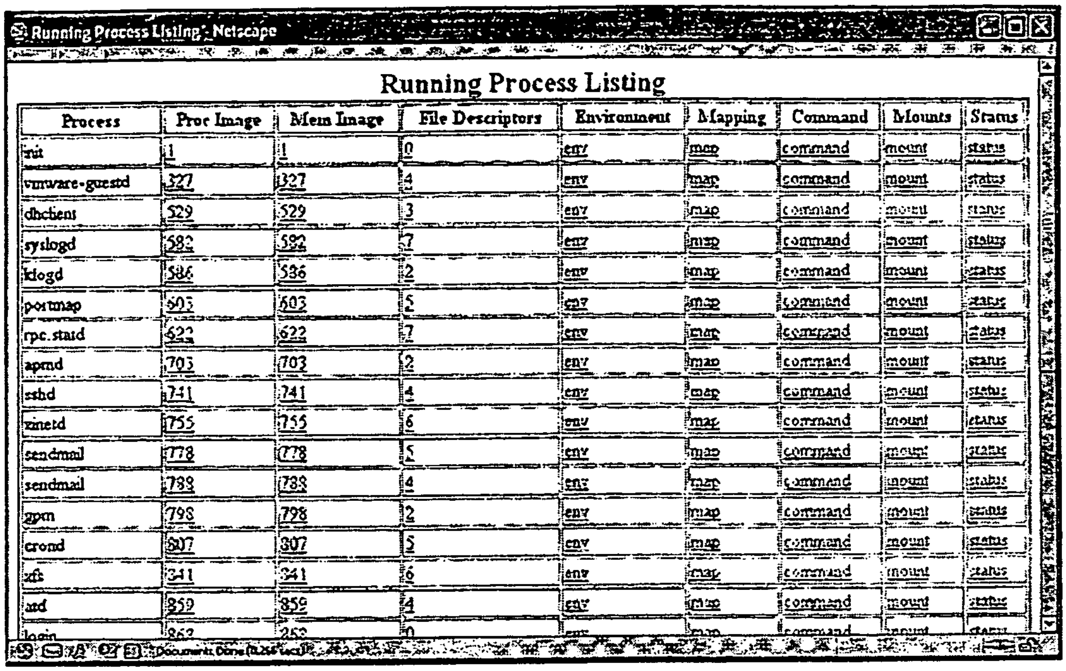


FIG. 29(h)



Running Process Listing

Process	Proc Image	Mem Image	File Descriptors	Environment	Mapping	Command	Mounts	Status
init	1	1	0	env	map	command	mount	status
vmware-guestd	327	327	4	env	map	command	mount	status
dhclient	529	529	3	env	map	command	mount	status
syslogd	582	582	7	env	map	command	mount	status
klogd	586	586	2	env	map	command	mount	status
portmap	603	603	5	env	map	command	mount	status
rpc.statd	622	622	7	env	map	command	mount	status
apmd	703	703	2	env	map	command	mount	status
sshd	741	741	4	env	map	command	mount	status
xinetd	755	755	6	env	map	command	mount	status
sendmail	778	778	5	env	map	command	mount	status
sendmail	788	788	4	env	map	command	mount	status
gpm	798	798	2	env	map	command	mount	status
crond	807	807	5	env	map	command	mount	status
xfs	841	841	6	env	map	command	mount	status
atd	859	859	4	env	map	command	mount	status
login	862	862	0	env	map	command	mount	status

FIG. 29(i)

267

269

```
total 13696
drwxr-xr-x    2 root      root          4096 Jan   5 19:41 .
drwxr-xr-x   11 root      root          4096 Jan   5 22:26 ..
-rwxr-xr-x    1 root      root         33960 Jan   5 19:40 1.exe
-rwxr-xr-x    1 root      root         33960 Jan   5 19:40 1.mem_exe
-rwxr-xr-x    1 root      root        103165 Jan   5 19:40 327.exe
-rwxr-xr-x    1 root      root        103165 Jan   5 19:40 327.mem_exe
-rwxr-xr-x    1 root      root        390950 Jan   5 19:40 529.exe
-rwxr-xr-x    1 root      root        390950 Jan   5 19:40 529.mem_exe
-rwxr-xr-x    1 root      root         33635 Jan   5 19:40 582.exe
-rwxr-xr-x    1 root      root         33635 Jan   5 19:40 582.mem_exe
-rwxr-xr-x    1 root      root         28571 Jan   5 19:40 586.exe
-rwxr-xr-x    1 root      root         28571 Jan   5 19:40 586.mem_exe
-rwxr-xr-x    1 root      root         40144 Jan   5 19:40 603.exe
-rwxr-xr-x    1 root      root         38147 Jan   5 19:40 603.mem_exe
```

FIG. 30(a)

```
fd: 0 READ-WRITE /socket:/[1103]
fd: 1 WRITE-ONLY /var/log/messages
fd: 2 WRITE-ONLY /var/log/secure
fd: 3 WRITE-ONLY /var/log/maillog
fd: 4 WRITE-ONLY /var/log/cron
fd: 5 WRITE-ONLY /var/log/spooler
fd: 6 WRITE-ONLY /var/log/boot.log
```

271

FIG. 30(b)

273

```
SSH_AGENT_PID=4606
HOSTNAME=sring-1.internal.vlan.iwc.sytexinc.com
PVM_RSH=/usr/bin/rsh
SHELL=/bin/bash
TERM=xterm
HISTSIZE=1000
GTK_RC_FILES=/etc/gtk/gtkrc:/root/.gtkrc-1.2-gnome2
WINDOWID=27270368QTDIR=/usr/lib/qt-3.1
USER=root
LS_COLORS=
PVM_ROOT=/usr/share/pvm3
SSH_AUTH_SOCK=/tmp/ssh-XX3BsOyB/agent.4542
SESSION_MANAGER=local/sring-1.internal.vlan.iwc.sytexinc.com:/tmp/.ICE-
unix/4542
USERNAME=root
MAIL=/var/spool/mail/root
PATH=/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin
:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin:/usr/local/netscape
INPUTRC=/etc/inputrc
PWD=/root
XMODIFIERS=@im=none
LANG=en_US.UTF-8
LAMHELPFILE=/etc/lam/lam-helpfile
GDMSESSION=Default
SSH_ASKPASS=/usr/libexec/openssh/gnome-ssh-askpass
HOME=/root
SHLVL=2X
PVM_ROOT=/usr/share/pvm3/xpvm
GNOME_DESKTOP_SESSION_ID=Default
BASH_ENV=/root/.bashrc
LOGNAME=root
LESSOPEN=|/usr/bin/lesspipe.sh %s
DISPLAY=:0.0G_
BROKEN_FILENAMES=1
COLORTERM=gnome-terminal
XAUTHORITY=/root/.Xauthority_=/usr/bin/ssh
```

FIG. 30(c)

275

```
rootfs / rootfs rw 0 0
/dev/root / ext3 ro 0 0
/proc /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /mnt/hgfs vmware-hgfs rw,nosuid,nodev 0 0
/dev/sdb1 /mnt vfat rw 0 0
```

FIG. 30(d)

277

```
Name:   vmware-guestd
State:  R (running)
Tgid:   327
Pid:    327
PPid:   1
TracerPid:        0
Uid:    0         0         0         0
Gid:    0         0         0         0
FDSize: 32
Groups:
VmSize:      1424 kB
VmLck:          0 kB
VmRSS:        444 kB
VmData:        48 kB
VmStk:          8 kB
VmExe:         84 kB
VmLib:       1252 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000000000
SigCgt: 0000000000004a07
CapInh: 0000000000000000
CapPrm: 00000000fffffeff
CapEff: 00000000fffffeff
```

FIG. 30(e)

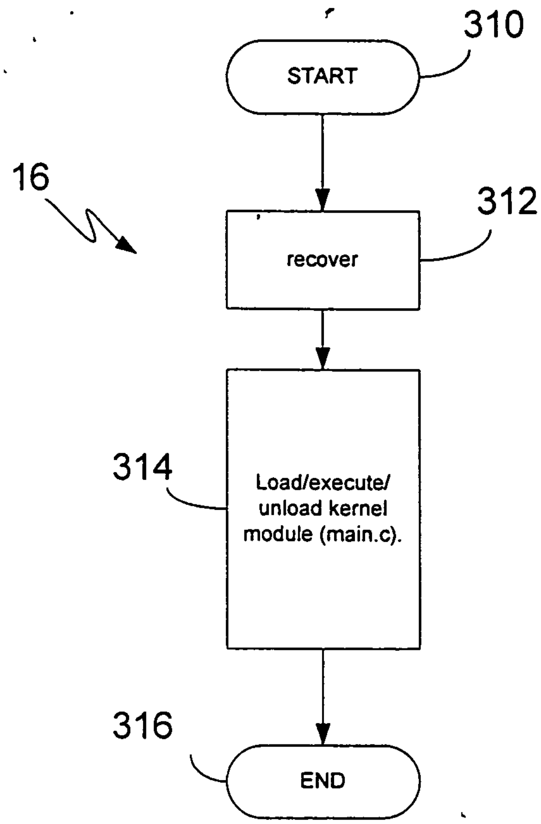


FIG. 31

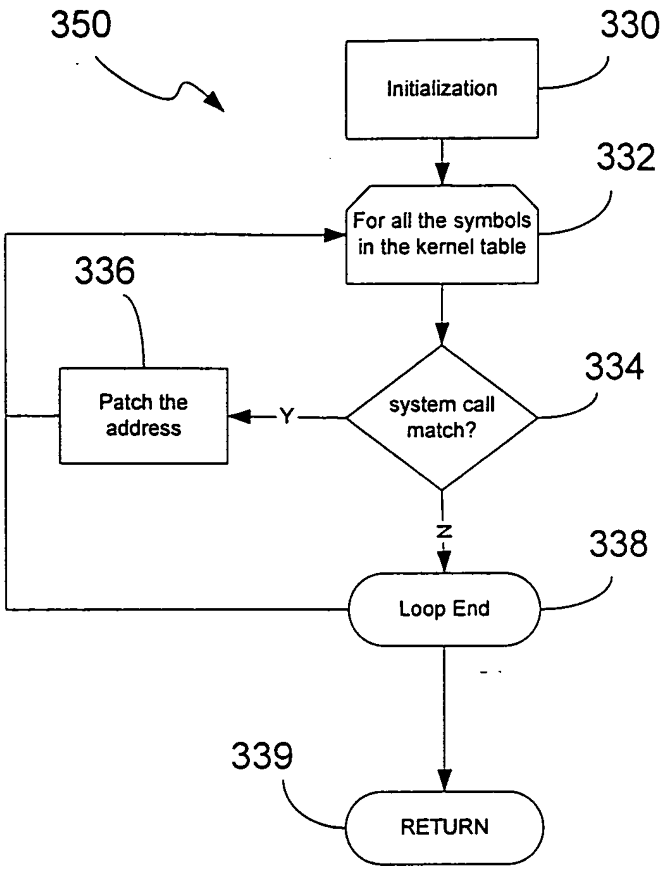


FIG. 33

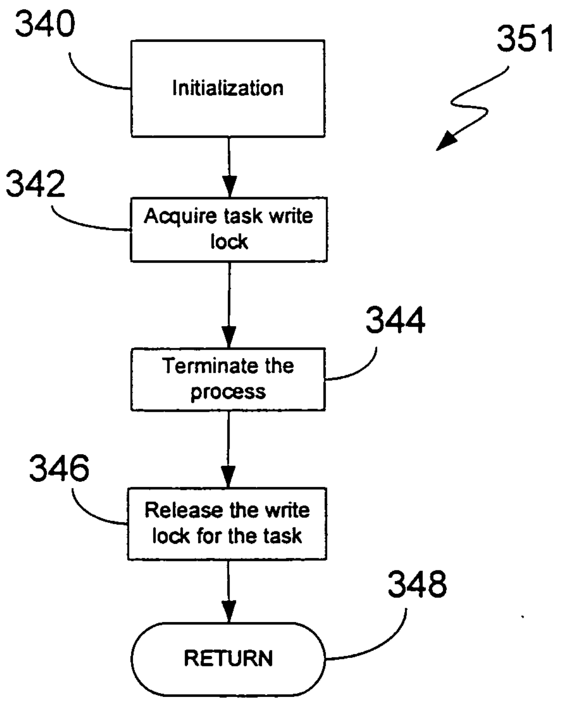


FIG. 34

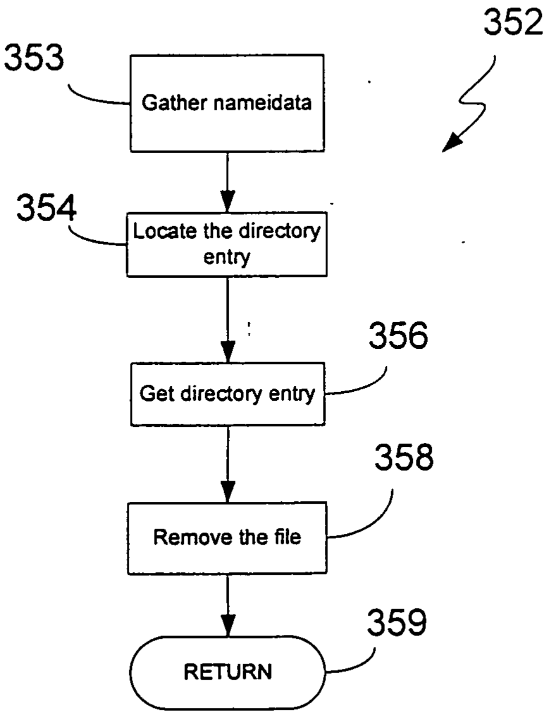


FIG. 35

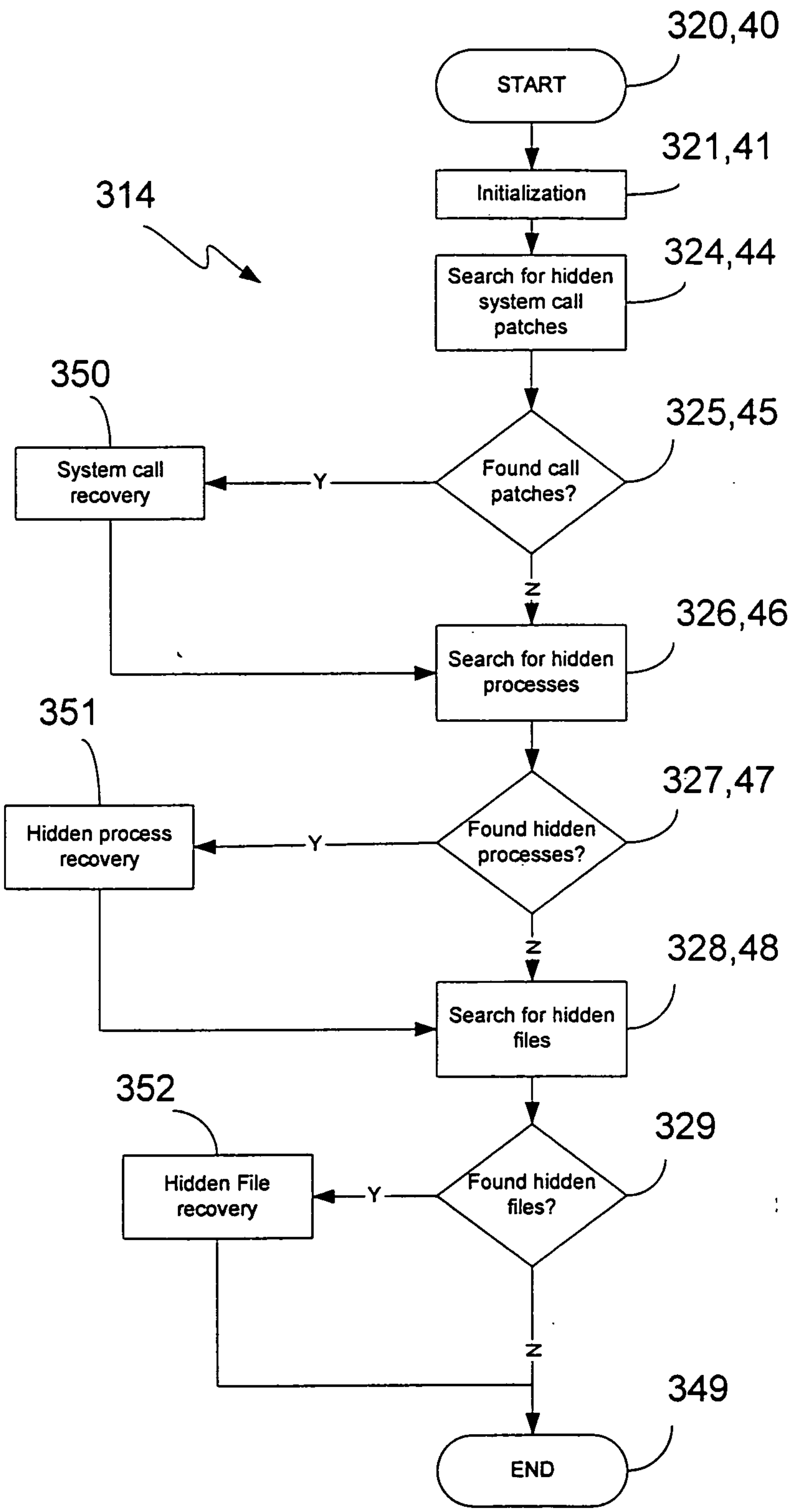
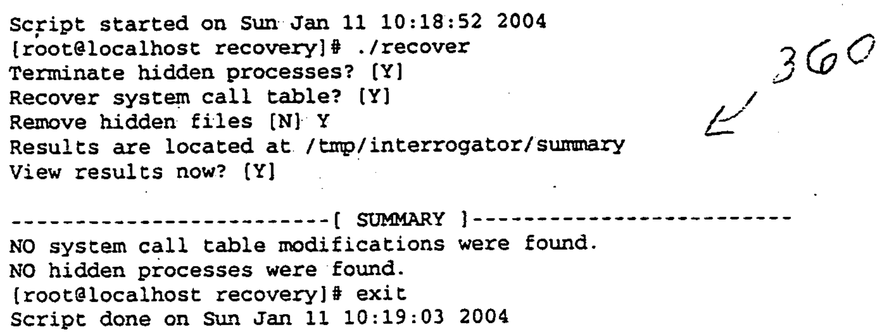
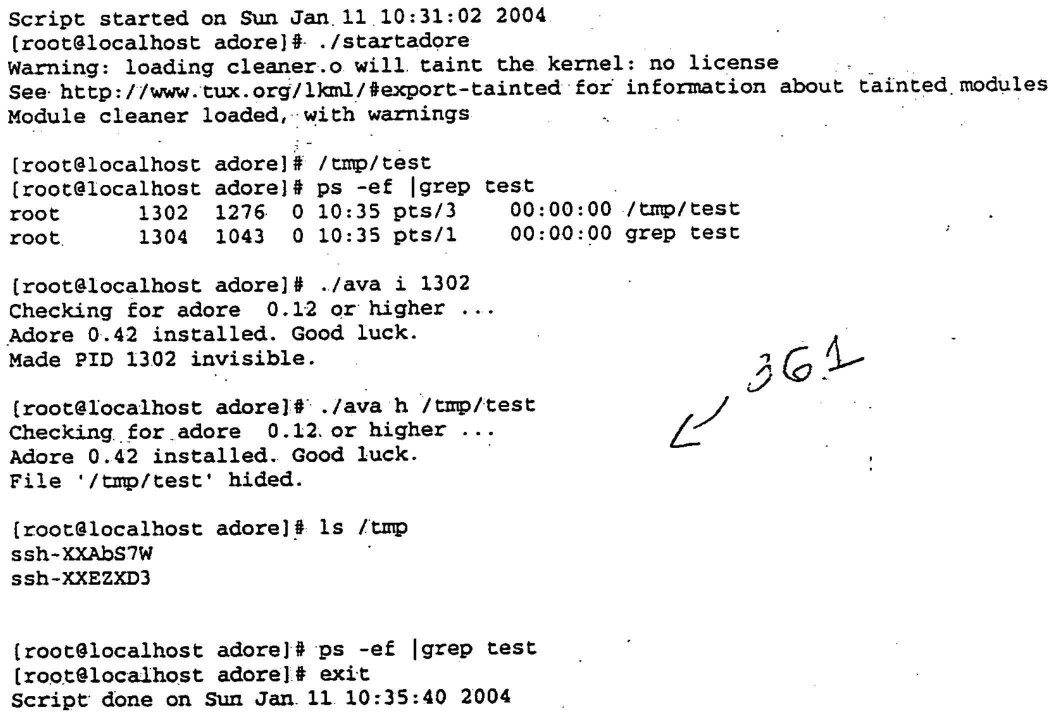

320,40
START
321,41
Initialization
314
324,44
Search for hidden system call patches
350
325,45
System call recovery
Y
Found call patches?
N
326,46
Search for hidden processes
351
327,47
Hidden process recovery
Y
Found hidden processes?
N
328,48
Search for hidden files
352
329
Hidden File recovery
Y
Found hidden files?
N
349
END

FIG. 32



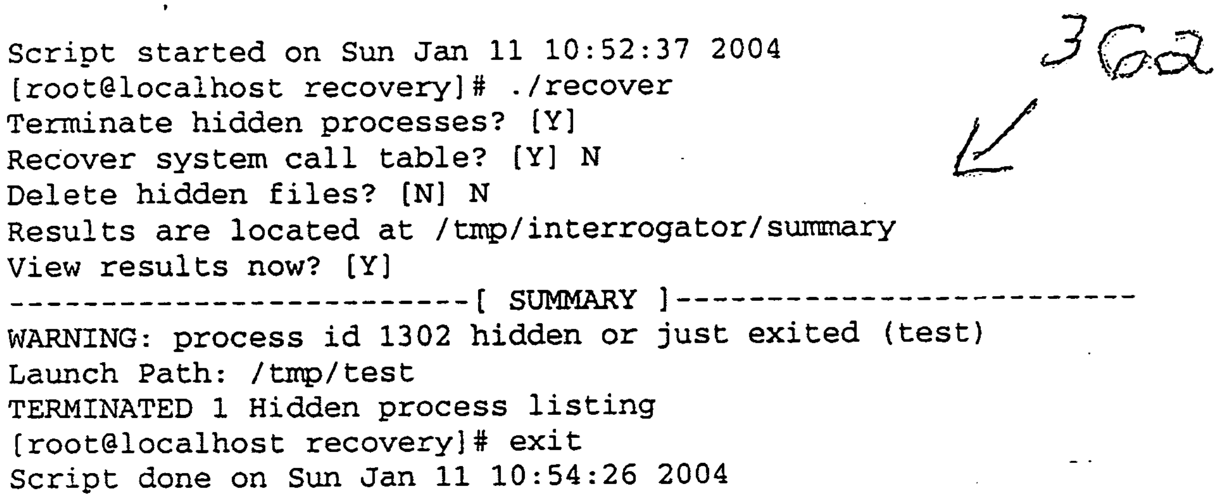
```
Script started on Sun Jan 11 10:18:52 2004
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y]
Recover system call table? [Y]
Remove hidden files [N] Y
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
NO system call table modifications were found.
NO hidden processes were found.
[root@localhost recovery]# exit
Script done on Sun Jan 11 10:19:03 2004
```

FIG. 36(a)



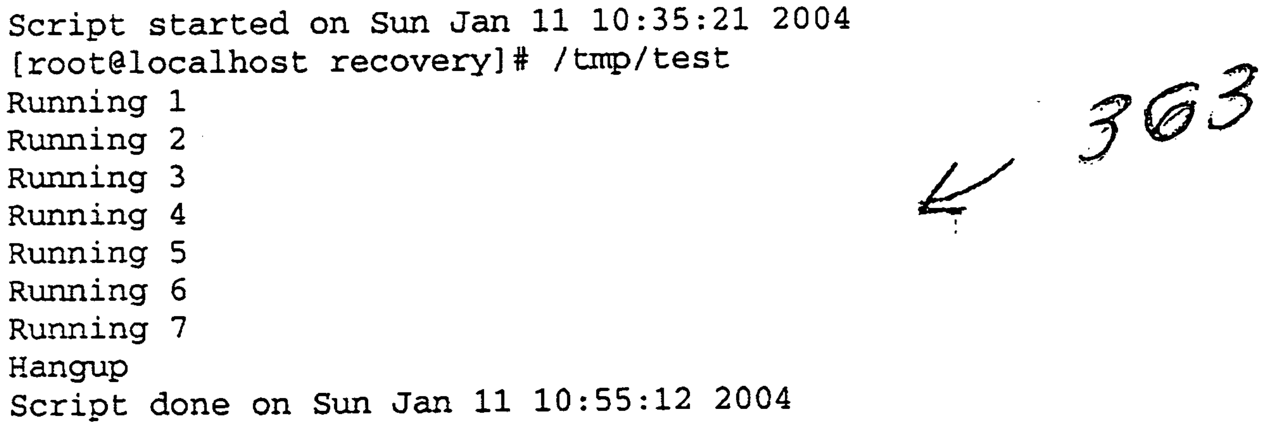
```
Script started on Sun Jan 11 10:31:02 2004
[root@localhost adore]# ./startadore
Warning: loading cleaner.o will taint the kernel: no license
See http://www.tux.org/lkml/#export-tainted for information about tainted modules
Module cleaner loaded, with warnings

[root@localhost adore]# /tmp/test
[root@localhost adore]# ps -ef |grep test
root      1302  1276  0 10:35 pts/3    00:00:00 /tmp/test
root      1304  1043  0 10:35 pts/1    00:00:00 grep test

[root@localhost adore]# ./ava i 1302
Checking for adore  0.12 or higher ...
Adore 0.42 installed. Good luck.
Made PID 1302 invisible.

[root@localhost adore]# ./ava h /tmp/test
Checking for adore  0.12 or higher ...
Adore 0.42 installed. Good luck.
File '/tmp/test' hided.

[root@localhost adore]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3


[root@localhost adore]# ps -ef |grep test
[root@localhost adore]# exit
Script done on Sun Jan 11 10:35:40 2004
```

FIG. 36(b)



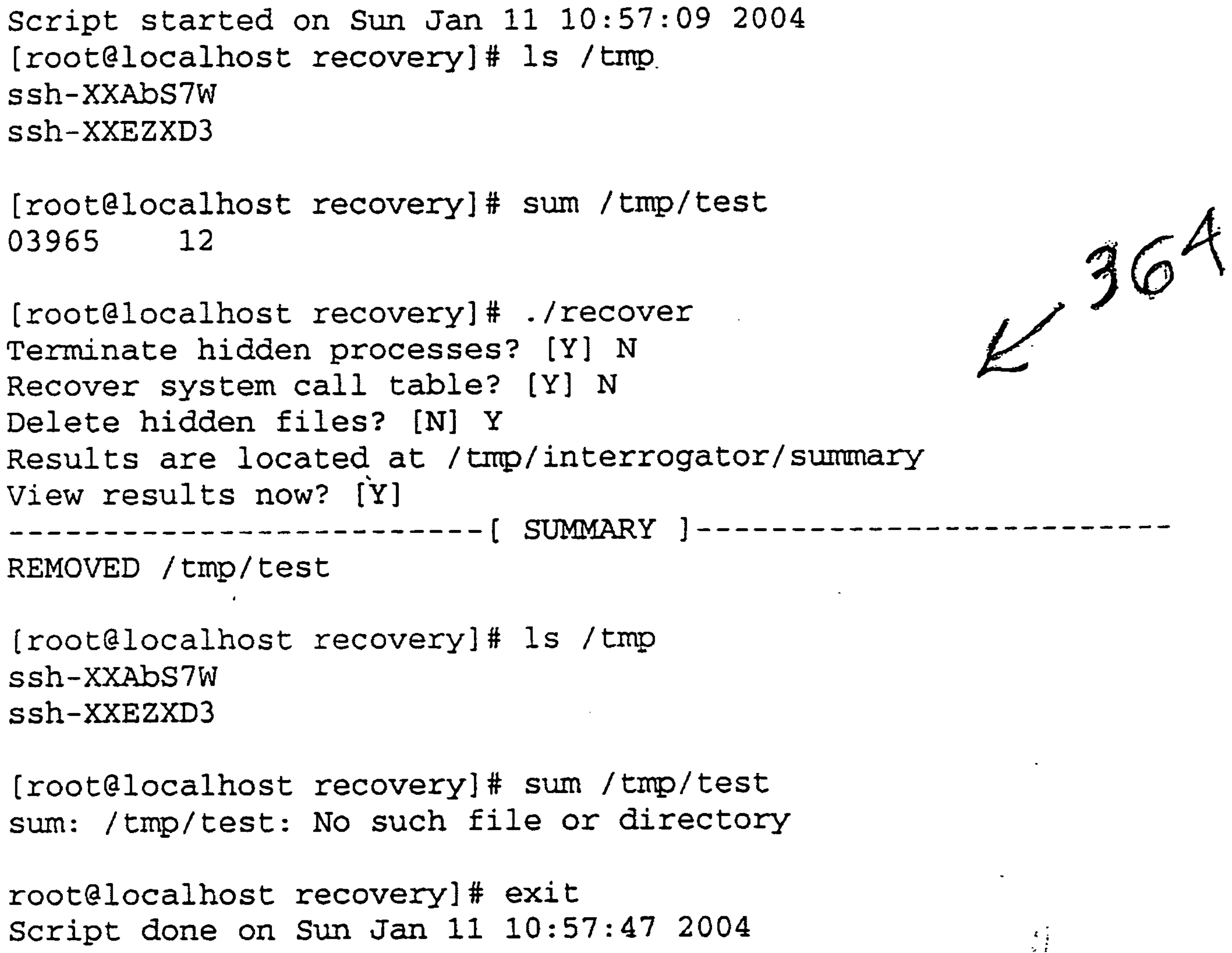
```
Script started on Sun Jan 11 10:52:37 2004
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y]
Recover system call table? [Y] N
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary
View results now? [Y]
-------------------------[ SUMMARY ]-------------------------
WARNING: process id 1302 hidden or just exited (test)
Launch Path: /tmp/test
TERMINATED 1 Hidden process listing
[root@localhost recovery]# exit
Script done on Sun Jan 11 10:54:26 2004
```

FIG. 36(c)



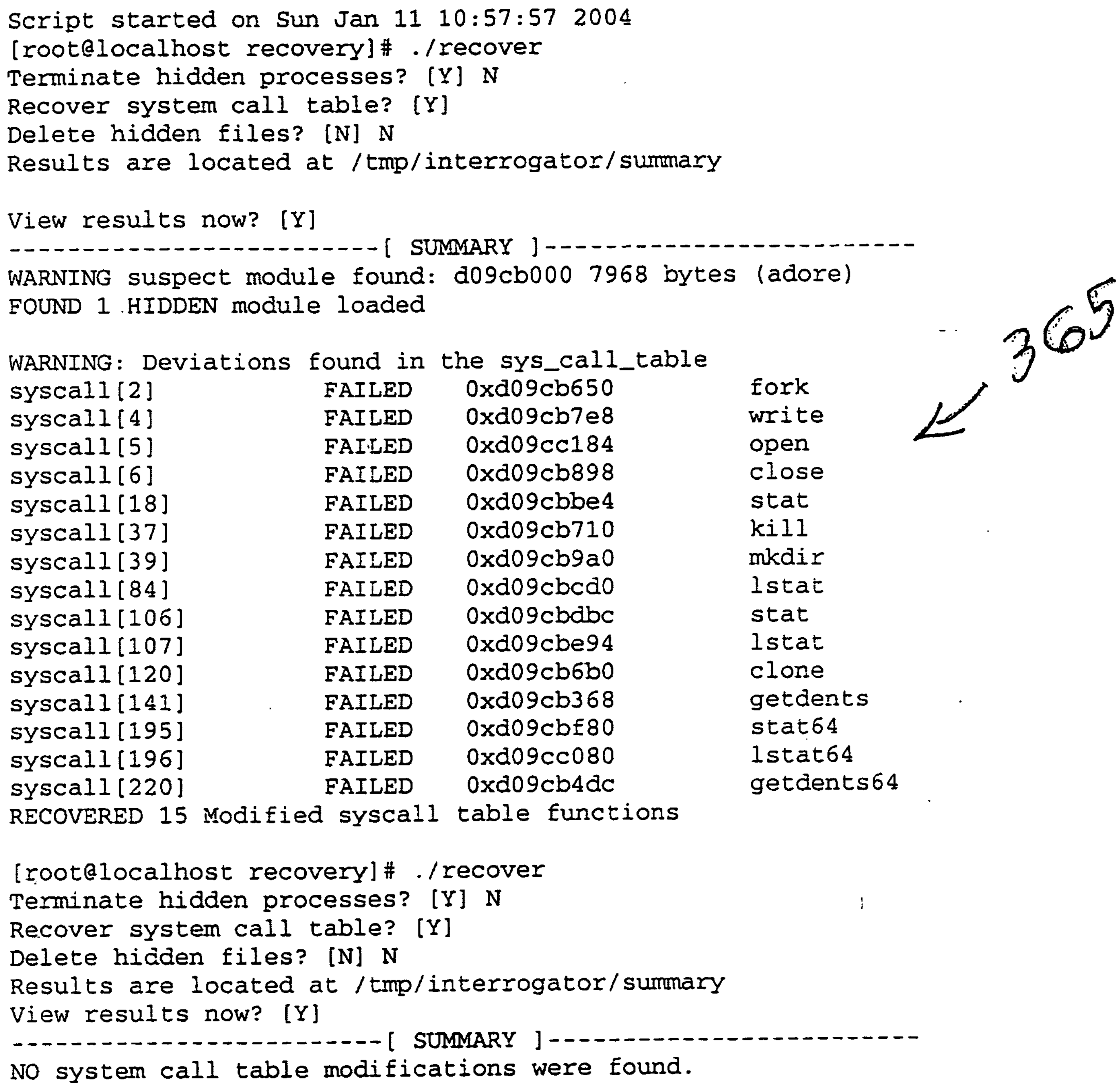
```
Script started on Sun Jan 11 10:35:21 2004
[root@localhost recovery]# /tmp/test
Running 1
Running 2
Running 3
Running 4
Running 5
Running 6
Running 7
Hangup
Script done on Sun Jan 11 10:55:12 2004
```

FIG. 36(d)



```
Script started on Sun Jan 11 10:57:09 2004
[root@localhost recovery]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3

[root@localhost recovery]# sum /tmp/test
03965    12

[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y] N
Delete hidden files? [N] Y
Results are located at /tmp/interrogator/summary
View results now? [Y]
-------------------------[ SUMMARY ]-------------------------
REMOVED /tmp/test

[root@localhost recovery]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3

[root@localhost recovery]# sum /tmp/test
sum: /tmp/test: No such file or directory

root@localhost recovery]# exit
Script done on Sun Jan 11 10:57:47 2004
```

FIG. 36(e)



```
Script started on Sun Jan 11 10:57:57 2004
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y]
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary

View results now? [Y]
-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: d09cb000 7968 bytes (adore)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]          FAILED    0xd09cb650      fork
syscall[4]          FAILED    0xd09cb7e8      write
syscall[5]          FAILED    0xd09cc184      open
syscall[6]          FAILED    0xd09cb898      close
syscall[18]         FAILED    0xd09cbbe4      stat
syscall[37]         FAILED    0xd09cb710      kill
syscall[39]         FAILED    0xd09cb9a0      mkdir
syscall[84]         FAILED    0xd09cbcd0      lstat
syscall[106]        FAILED    0xd09cbdbc      stat
syscall[107]        FAILED    0xd09cbe94      lstat
syscall[120]        FAILED    0xd09cb6b0      clone
syscall[141]        FAILED    0xd09cb368      getdents
syscall[195]        FAILED    0xd09cbf80      stat64
syscall[196]        FAILED    0xd09cc080      lstat64
syscall[220]        FAILED    0xd09cb4dc      getdents64
RECOVERED 15 Modified syscall table functions

[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y]
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary
View results now? [Y]
-------------------------[ SUMMARY ]-------------------------
NO system call table modifications were found.
```

FIG. 36(f)

```
Script started on Sun Jan 11 11:31:47 2004
[root@localhost adore]# ps -ef |grep test
root      1284  1258  0 11:31 pts/1    00:00:00 /tmp/test

[root@localhost adore]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3
test

[root@localhost adore]# ./startadore
Warning: loading cleaner.o will taint the kernel: no license
See http://www.tux.org/lkml/#export-tainted for information about tainted modules
Module cleaner loaded, with warnings

[root@localhost adore]# ./ava i 1284
Checking for adore  0.12 or higher ...
Adore 0.42 installed. Good luck.
Made PID 1284 invisible.

[root@localhost adore]# ./ava h /tmp/test
Checking for adore  0.12 or higher ...
Adore 0.42 installed. Good luck.
File '/tmp/test' hided.

[root@localhost adore]# ps -ef |grep test
[root@localhost adore]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3

[root@localhost adore]# cd ../interrogator/recovery
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y] Y
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary
View results now? [Y]
-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: d09cb000 7968 bytes (adore)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]          FAILED    0xd09cb650        fork
syscall[4]          FAILED    0xd09cb7e8        write
syscall[5]          FAILED    0xd09cc184        open
syscall[6]          FAILED    0xd09cb898        close
syscall[18]         FAILED    0xd09cbbe4        stat
syscall[37]         FAILED    0xd09cb710        kill
syscall[39]         FAILED    0xd09cb9a0        mkdir
syscall[84]         FAILED    0xd09cbcd0        lstat
syscall[106]        FAILED    0xd09cbdbc        stat
syscall[107]        FAILED    0xd09cbe94        lstat
syscall[120]        FAILED    0xd09cb6b0        clone
syscall[141]        FAILED    0xd09cb368        getdents
syscall[195]        FAILED    0xd09cbf80        stat64
syscall[196]        FAILED    0xd09cc080        lstat64
syscall[220]        FAILED    0xd09cb4dc        getdents64
RECOVERED 15 Modified syscall table functions

[root@localhost recovery]# ps -ef |grep test
root      1284  1258  0 11:31 pts/1    00:00:00 /tmp/test
root      1345  1288  0 11:33 pts/2    00:00:00 grep test

[root@localhost recovery]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3
test

[root@localhost recovery]# exit
Script done on Sun Jan 11 11:33:21 2004
```

300

FIG. 36(g)